

# Health IT Joint Committee Collaboration

A Joint Policy and Standards Public Advisory Body on Health Information Technology  
to the National Coordinator for Health IT



## Health IT Joint Committee Collaboration Application Program Interface Task Force Hearing Final Transcript January 26, 2016

### Presentation

#### Operator

All lines are bridged.

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

Thank you. Good afternoon everyone, this is Michelle Consolazio with the Office of the National Coordinator. This is a meeting of the Joint Health IT Policy and Health IT Standards Committee's API Task Force. This is a public meeting and there will be time for public comment at the end of today's call. As a reminder, please state your name before speaking as this meeting is being transcribed and recorded. I will now take the role. Meg Marshall? I know Meg is here. Josh Mandel?

#### Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School

Hi, Michelle; I am here.

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

Hi, Josh. Aaron Miri?

#### Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center

Hello.

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

Hi, Aaron. Aaron Seib? David Yak? Drew Shiller?

#### Drew Schiller – Chief Technology Officer & Co-Founder – Validic

Here; hi, Michelle.

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

Hi, Drew. Ivor Horn? Leslie Kelly Hall?

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Here.

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

Hi, Leslie. Linda Sanches?

**Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services**

Here.

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

Hi, Linda.

**Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services**

Hello.

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

Rajiv Kumar?

**Rajiv B. Kumar, MD – Clinical Assistant Professor of Pediatric Endocrinology & Diabetes - Stanford University School of Medicine**

Here; good morning.

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

Hi, Rajiv. Richard Loomis? Robert Jarrin? And from ONC do we have Rose-Marie Nsahlai?

**Rose-Marie Nsahlai – Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology**

Here, Michelle.

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

Hi, Rose-Marie. Okay, we are getting a little bit of feedback, I am not sure who it is from, but we will hopefully fix that. So, thank you all for joining. I just want to go over some administrative items before we get started and I will hand it to Josh and Meg. A reminder to our task force members, when we open it up to the queue to ask questions, if you could please use the hand-raising feature; you will find that hand-raising feature at the top of your screen, there is a little man with his hand raised. You just click on that and that will put you in the queue to ask questions.

A reminder to all of our panelists, if you could please keep your remarks to five minutes it would be appreciated. If you go too much over, I will ask you to wrap up. And just as a reminder of how today will go, we will have all the panelists from panel one share their testimony and then we will open it up to questions from our task force, and then we will go to panel two. For our task force members, if you want

to be reminded about the questions that the panelists were asked, it was included in today's agenda at the back, on the second page of the agenda. And so with that, I will turn it over to Meg and Josh.

**Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

All right, this is Josh Mandel. Thanks very much Michelle and thank you especially to our panelists for joining us for today's testimonies; really happy to have such a diverse group of experts in the field today with us for this, first of two sessions of public hearing. And I just want to briefly highlight the two panels that we will have today focusing on consumer technology.

And for folks who want to have a sense then and for folks especially who are listening in public of what the questions are that we have asked of our panelists, just want to make sure that I can set the stage by saying, we are really asking for panelists to share their expertise with what it takes to deploy APIs in the real world, what some of the security threats and vulnerabilities are that real-world deployments have to think about.

Where the differences are between healthcare related APIs and general kinds of API access that consumers would use in other areas of their everyday life and try to get a sense in terms of healthcare APIs, what kind of applications are using these data downstream and what kinds of protection are put in place on behalf of consumers and also on behalf of the healthcare provider organizations that are often supplying these data.

So, I think I will keep the opening remarks just brief and to those, and say that I am really excited to hear from panelists today and to engage in some dialogue as well. And with that, I think I will turn it back over to Meg, if you have got anything to say or back to Michelle.

**Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation**

This is Meg Marshall; Josh thanks for that. Nope, I do not have nothing to add just to simply to enforce how excited I am and how valuable I think the comments that we are going to hear over the next couple of days will be...thanks again for your time.

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

Yes, okay; so thank you. And so we will get started with panel one. First let me just make sure that everyone is here. I apologize in advance if I butcher your name, hopefully you will correct me. So on panel one we have David Wollman from NIST; David, are you here?

**David Wollman, PhD – Deputy Director, Smart Grid and Cyber-Physical Systems Program Office – National Institute of Standards and Technology**

Yes I am.

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

Okay. Stephan...I'm not going to even say your last name, I am going to let you say it, from Google.

**Stephan Somogyi – Product Manager, Security and Privacy – Google**

Somogyi and yes, I am here.

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

Somogyi, okay; h, Stephan. David Ting?

**Stephan Somogyi – Product Manager, Security and Privacy – Google**

Hi there.

**David Ting – Co-Founder and Chief Technology Officer – Imprivata**

Yes, this is David.

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

Hi, David. Greg Brail?

**Gregory Brail – Chief Architect – Apigee**

Yes, this is Greg.

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

Hi, Greg. And Eve Mahler?

**Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock**

Yes, I am here; hi.

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

Hi. Okay, so David, if you are ready, you can kick us off and we will get started.

**David Ting – Co-Founder and Chief Technology Officer – Imprivata**

All right.

**David Wollman, PhD – Deputy Director, Smart Grid and Cyber-Physical Systems Program Office – National Institute of Standards and Technology**

Thank you.

**David Ting – Co-Founder and Chief Technology Officer – Imprivata**

The other David.

**David Wollman, PhD – Deputy Director, Smart Grid and Cyber-Physical Systems Program Office – National Institute of Standards and Technology**

This is...my name is David Wollman and I am also joined by my colleague Marty Burns. Both of us work at the National Institute of Standards and Technology, part of the US Department of Commerce and we are delighted to be here this afternoon to provide some information on the Green Button Initiative in the Energy Space that is relevant to your conversation here today on APIs and healthcare. I was originally going to participate on the second panel, but due to some schedule constraints, moved to the first so I will answer a mix of questions between the panels. Next slide, please.

The Green Button Initiative is a secure way to communicate energy usage information electronically using standardized, RESTful API web services and a common data format. You will note that we are inspired by the Blue Button Initiative in health and that we have modeled some of our activity after Blue Button including working closely with the federal government, with the White House, the Department of Energy, and many industry partners. We have developed some innovative approaches in web technologies for Green Button, building on existing best practices including Atom Publishing and OAuth2, and I will mention these a bit too later. These advances enable Green Button perhaps to serve as useful pattern for other data initiatives facing similar issues.

In short, the goal of the Green Button Initiative is to work with industry to increase consumer access to their own energy usage information data supported by an ecosystem of Green Button standards, testing and certification, developer support tools and applications and services. Our status is that with voluntary adoption by many utilities nationwide, over 60 million US customers, representing over 100 million citizens and over 2.6 million Canadian customers now have Green Button access, such as that shown on the utilities website on the bottom right of the slide. Next slide, please.

We have worked with numerous partners to create the Green Button ecosystem which include the key pillars of standards, example code and testing and certification which includes the standing up of a nonprofit trade alliance, the Green Button Alliance under the UCAIug international users group, and also testing and certification by Underwriters Laboratory with accreditation by ANSI, the American National Standards Institute. So this is an example in which we have created a more complete testing and certification program that might be of interest to folks in the health space.

NIST has worked with all of these partners to support the standards development process and the test development, including testing and certification tools and an API developer sandbox. I should mention that the certification capability is not fully in place yet and we need more engagement with Apps developers to really make this more of a vibrant ecosystem.

One point I would like to make with respect to healthcare is that this work is done in voluntary cooperation with the energy industry. Within Smart Grid, we do not have the legislative authority model for a federal government driven testing and certification regime, but we have been quite successful in working with industry. Next slide, please.

Let us talk just a bit about data structure. The data in energy usage is inherently complex at a point of measurement such as a usage point there are multiple measurements, some are instantaneous, some are intervals such as energy. Information models are typically defined and presented in class diagrams, as shown here using Unified Modeling Language. Classes represent data structures and class diagrams present the data structures and the relationship between the classes.

Two standards that have been helpful for exchange of complex data are XML and Atom Syndication. Combined they provide an algorithmic transformation of an information model in UML to a parsable data set exchangeable by web service. And since data can be arbitrarily complex and exchanging it as a single chunk may be inefficient, you may want to dive in and get one piece of the data, the Atom Syndication Format provides a means of simplifying the structure by flattening it into a sequence of entry fragments, such as shown on the right-hand side. Next slide, please.

In energy usage information exchange in Green Button, there are three principal roles; there is a data custodian, which is often the electric utility; there is the third-party, the entity that wishes to provide a

service to a retail customer and wants access to the data; this is often an Apps developer, and also the retail customer, the party who the data is about and wants to benefit from an analysis of their data. All Green Button exchanges share a basic data format in common. In Download My Data, this data is exchanged by an interaction between the retail customer and the data custodian on the data custodian's web portal; result is an XML file which is downloaded and can be used however the recipient sees fit.

The more interesting case is Green Button Connect My Data, involving the authorization and subsequent automated transfer of data via secure, RESTful web services, with the ability by the retail customer to modify access later as needed. The kind of API that was is a resource-oriented architectures where complex data structures can be navigated by a path URIs and also query parameters used to filter the results. The attractiveness of these architectures is that once the data structures are understood, the API could be used for new purposes not originally envisioned. Next slide, please.

Now let's get into some details. Authentication identifies a client to the server and allows communications over a secure channel and authorization identifies access rights to an authenticated party. The authorization of the third-party to the retail customer-held...resources held by data custodian is what OAuth2 is designed for and is widely used in industry.

The key principle of OAuth is that the data custodian and the third-party should never exchange private information about the retail customer between them. This is achieved through clever use of web browser redirection, and I won't get into the details of it. I do want to note however that the requirements are not symmetrical. Typically the data custodian has the responsibility to maintain the privacy and access to the retail customer's data and therefore must strongly authenticate the customer's response. On the other hand, the third-party may have a very short-term and, you know casual relationship to the retail customer and may not need strong authentication.

A key point in the...

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

Could you please wrap up?

**David Wollman, PhD – Deputy Director, Smart Grid and Cyber-Physical Systems Program Office – National Institute of Standards and Technology**

Certainly. On the right-hand side we see some information that was done with consultation with our NIST colleagues. Next slide.

On this, we have done some unique work on scope negotiation and extended OAuth to allow long-lived authorization; that is something maybe we can take up in the questions. Next slide.

And finally we have a nice set of web resources that are available and listed here, including an API sandbox and much more. So with that I will conclude and pass it back to the moderator.

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

Thank you, David. Stephan if you ready?

**Stephan Somogyi – Product Manager, Security and Privacy – Google**

Yes, hi. My name is Stephan Somogyi and I am member of Google's Core Security team. I would like to thank you all for the opportunity to provide input into this process. I would like to focus my initial comments on two primary categories; the protection of data and API engineering.

We can view the protection of data really twofold; there is protection of the data itself and protecting access to it. Protecting the data is itself most efficiently done via encryption, both at rest for the data that is stored somewhere and in transit, while it traverses networks, including the Internet. Google has for many years' promulgated best practices around the implementation of encryption, key management for the encryption and making sure that we make decisions that are pragmatic for the entire ecosystem. But this work comes at a cost.

Any organization wishing to not only adhere to the best practices but also make sure that all its partners adhere to it must allocate the resources to not merely maintain the systems, but to perform continuation engineering and make sure that all the systems are always following the best practices of the time, and not just the ones that were current at the time of the RFP.

Data in transit should be protected by best practice implementations of encryption standards. They should be protected by modern browsers used the current versions that support the client side of these implementations. And they should also integrate best practices around certificate managements including features like certificate pinning and validation of certificates via mechanisms like certificate transparency. The protection of data at rest should be careful to encrypt the data well, and this includes key management and also to provide the availability and high speed of access.

It is important to note that the technical controls are necessary, but not sufficient to building an overall secure system. The hosting party of the data must have sufficient internal process and policy controls and organizational security programs to assure a common and high level of training and knowledge about the issues that create risk.

Security overall we feel needs to be considered holistically and systematically. It is straightforward to implement something that is fully buzz word compliant, and even blessed by standards body, but at the same time it is woefully inadequate in the real world. The web standard for encryption in the early days of Wi-Fi is an excellent example of this; we must not repeat these errors. Mechanisms in place should guarantee security of the data as well as its integrity to make sure that an adversary cannot tamper with it. In a healthcare context, such modification, either deliberate or as a result of errors could have quite literally lethal consequences.

Now in a greater context here, it is important to understand that APIs are not uniquely insecure or uniquely vulnerable. Any time you have a system that is open to the Internet at large; you are subject to the vagaries of such a diverse environment. APIs can and should be designed to minimize the impact of coding errors or security incidents. Where appropriate, devices involved should check cryptographic signatures on new firmware and/or software, or implement protocols that limit the data that is being sent around to perhaps only diagnostic data that doesn't allow triggering of any kind of high risk to human actions.

Now while encryption is one mechanism to enforce appropriate access to data, setting up appropriate and manageable permission systems is also really important. Data should be accessible only to those with a need to have access and the accessibility of the data should also be validated on an ongoing basis

to make sure that everyone who has access still needs it. API engineering fundamentally needs to be a manifestation of best engineering practices. Such practices create incentive structures and an engineering culture where correctness and resilience of implementation is paramount. A healthy engineering culture provides the preconditions for design patterns that make secure implementation of API a matter of course rather than an anomaly.

Data from the outside should be considered untrusted; doing so eliminates common attack vectors like sequel injection and so forth. I have a colleague who this week is giving a talk at OAuth in California to discuss an approach, in detail; these types of practices based on our own hard won experiences. So, this information is available, it is out there and it is accessible to everybody. Thank you very much.

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

Thank you. David Ting?

**David Ting – Co-Founder and Chief Technology Officer – Imprivata**

All right; I am joined here by my colleague, Arny Epstein, who is the Chief Engineer for Imprivata. I'd like to thank the task force for providing Imprivata with the opportunity to testify before the task force and give insight into the efforts our company is making to improve the patient experience. I am David Ting; I am the Co-Founder and Chief Technology Officer at Imprivata.

Imprivata is a healthcare information technology company based in Lexington, Mass with more than 400 employees. We went public in 2014. Imprivata provides authentication, access management and patient identification. We seek to enhance the healthcare experience by streamlining the provider authentication process.

I am here today to testify before the task force and present insight into the use of APIs for the interchange of data between healthcare providers and between providers and patients. APIs have been in commercial use over the Internet since the late 1990s when they were given the name, web services. By the early 2000's, techniques for creating secure Internet APIs became mature enough that companies like Salesforce, eBay and Amazon were able to issue secure APIs. The banking industry uses secure Internet APIs for fund transfers among other interbank transactions.

There many best practices that are not unique to healthcare. In particular, there are five areas that concerns Imprivata when dealing with the securities for computer interactions. These include: Confidentiality: When the data is exchanged, it must be done confidentially so it cannot be read while in transit between the sender and the receiver. Integrity: Integrity of the data being exchanged must remain. There should be assurances that the received data has not been altered in any way.

Availability: Security must cover prevention against attackers that would render the API inaccessible by authorized users. This is often called denial of service. Privacy: Assuring that the requesting party does not receive personal information beyond that which has been authorized by subject of the data; for an API, especially in healthcare, establishing the identity of the provider and permission of the patient are both critical to meeting privacy requirements. Multifactor authentication for example, is required for law enforcement officers to access the FBI's Criminal Justice Information System, or CJIS. Similar authentication requirements are necessary for healthcare to ensure the information is not being inappropriately accessed.

Finally, authentication and authorization in showing that the requesting party of the API has been authenticated by an identity provider service that is trusted, typically cryptographically, by the API issuer and that the requesting party has been granted the right to use of the API. Plus the reverse, that the requesting party can verify that the API service it is calling is authentic and not being impersonated.

Imprivata's role is to ensure that as an issuer of the API, it won't fall victim to malicious activity resulting in an attack or compromising its data sources. An API can assure it is not...it won't be used as a tool for malicious activity by following best practices the same way as a web application issuer does. Many of these are outlined by NIST, the National Institute of Standards and Technology in their special publications.

Compliance with best practices, code reviews, security reviews, automated code analysis and extensive testing are all commonly used and effective methods. Imprivata goes to great lengths to ensure that APIs are distributed in a way that ensures authenticity. APIs are distributed using public key cryptography. The solution is the same one as used to allow us to trust our banking and e-commerce sites today.

While Imprivata is not familiar with any existing broad adopted metrics for measuring maturity of an API, there are tools that aid in third-party access. There are hundreds of tools and frameworks and forms available regarding building secure APIs. The public sector security and development community are continually vetting these offerings. The fact that most organizations provide source code to a broad technical community means that it is feasible to automatically analyze the security of the codes.

Imprivata is not aware of any direct compliance implications for the use of APIs. If an API operates within a regulated environment such as healthcare, banking, etcetera, then its designs and testing must ensure that it complies with the relevant requirements.

Imprivata is aware of actual security concerns and is taking significant measures to combat the barriers to the adoption of APIs. We believe that risks can be mitigated through compliance with best practices and as...such as code reviews, security reviews, automated code analysis and extensive testing.

Thank you for having me here today. I look forward to our conversation and welcome any questions that you might have. Thank you.

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

Thank you, David. Greg Brail?

**Gregory Brail – Chief Architect – Apigee**

Hello, hi there; hopefully you can hear me okay now.

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

We can hear you.

**Gregory Brail – Chief Architect – Apigee**

Thanks. I am Greg Brail; I am the Chief Architect of Apigee. Apigee is a company that provides software and solutions that help organizations create, expose and consume APIs. And thanks for giving us the

opportunity to come here to address the community regarding the opportunities and issues presented by the adoption of APIs.

In the last 10 years, we have seen the idea of a web API grow from an experiment created by small numbers of web companies like Flickr and Yahoo to a technique used by popular social network mobile applications to a mainstream set of technologies and best practices that are being used across the industry to make it any easier for software developers to access data and services.

The very first web APIs like the early Yahoo Maps and Weather APIs, they might have been used for non-sensitive information, but that quickly changed. Today we see APIs being used for everything from mobile payment to healthcare to wholesale financial services. It is important to know that the API, at its simplest level is a contract. The contract specifies how a software developer accesses the API and tells the developer what to expect in return.

A well-designed API makes this contract very clear through documentation and specifications that describe not only what kind of request the API expects, but what kind of security controls have been put in place and what kind of security credentials the developer must acquire and present before he or she builds an application that uses the API.

Because an API is a contract, it is possible for the organization that offers the API to fully document and understand the interaction between the application that uses the API and the API itself. There are a number of tools and techniques available, we have already heard of some of them on this call, both from commercial software vendors as well as from the open-source community and there is a lot of public domain and open-source information from companies like Google and Apigee and others that explain how to use these tools and how to use these techniques.

All of these tools and techniques can be used to ensure for instance, that API access is not allowed unless the client follows the contract. They can monitor API usage and gather data to understand exactly who is using the API and how. Since the API interaction model is contract driven, it makes it possible for the organization that provides an API to add policies and security controls on every interaction.

That means an API team can regulate which applications and end users are authorized to use an API, which parts of the API they are allowed to use, when they are allowed to use them, how many API calls they are allowed to make, what parts of the API they can access and maybe even subsets of individual data fields. The team can control things like putting a limit on the number of API calls that can be made. And finally, the team that manages and provides the API can follow an audit trail of API calls to understand exactly what the authorized API users did and what unauthorized attempts that may have been made.

Now I mention all of this in the context of contracts to contrast with other mechanisms for disseminating data or making services available, such as offering a web App or a file transfer mechanism or sharing information via e-mail or even printing things out.

Because an API is a contract, the team providing the API, like I say, can know exactly what is allowed. There is nothing, unlike a web App, which is typically a very complicated collection of JavaScript and HTML and CSS and other things, an API is extremely precise in what it allows. This in my opinion means that offering information of the type we are talking via an API or offering service as an API presents the opportunity, using these well-known tools and well-known techniques from some of the folks on this call

in order to make the organization who offers the API aware of exactly what is being done and there is actually an opportunity to have all the right levels of security via the API that in some ways is a little bit less risky than offering the same information via a raw website or some other mechanism.

So as a result, I think that APIs rather than being a new security risk they provide a well-documented and popular way for organizations to share access and data to services with third parties while maintaining strict security controls. And I think that that's what we are going to talk about today in detail and I am looking forward to participating. Thanks.

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

Thank you, Greg. And last but not least, Eve.

**Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock**

Thank you. Well thanks for this opportunity to address the panel this timely week, just before Data Privacy Day. My name is Eve Maler; I am responsible for Privacy and Consent Innovation at ForgeRock. I Chair the User Managed Access Group and I Co-Chair the HEART Group with Debbie Bucci.

Regarding APIs generally, web-based let organizations and their partner, Echo Systems achieve extreme data accessibility. The Internet of Things phenomenon of the last couple of years owes its existence largely to the several years old API economy. Regarding API security, it sounds like I agree with Greg, some feel that API security and API accessibility are at odds; in my opinion, they need not be.

Traditional IT security practices often give a false sense of security if they present the classic crunchy shell and chewy center. API management and security gateway solutions have greatly improved the picture by serving the API economy, including access control to ensure that only correct users and applications get through and rate limiting to catch denial of service attacks, even if the APIs are intended to be open to all.

Regarding API privacy, even the best protected API may be destructive of privacy by virtue of the data its messages carry and of course successful data access may expose the legitimate client and its operator to personal data. Now at some point we always enter the territory of what has become known as “the BLT sandwich.” This stands for business, legal and technical. Even in the realm of legal agreements, some innovative solutions are actually being proposed.

Regarding data provenance, when you are creating static data, tagging for provenance can work well. But what if an API endpoint is able to report out say, a live feed of data coming from a sensor for blood oxygen levels? The provenance is actually upstream from the data. So if the trustworthiness of the device and the API can be established, propositions for which the technology does in fact exist, tags could be added to metadata used in the on-boarding ceremonies of the device and the API to their respective service ecosystems.

Regarding the proposition of industry-standard APIs, now standardizing an API within an industry is valuable when it is desired to remove business and technical friction from interactions among industry players. FHIR is obviously one key example here. Others exist, such as the open bank API in the UK.

Regarding the OAuth technology and its cousins, for any API it is recommended to use standardized mechanisms for security, identity and consent. This is because doing this reduces complexity, enables

the bridging together of different data sources, tends to have fewer vulnerabilities through more thorough vetting and tends to have more commercial and open source implementations. OAuth and OpenID Connect and UMA exist to help standardize security, identity and consent interactions. Their specifications actually define standardized APIs within them and in circular fashion, are themselves designed for use with other APIs, both proprietary and industry-standard.

OAuth has innovated a great deal around consent, authorization and revocation. However, OAuth revocation is coarse-grained and OAuth consent doesn't actually greatly empower the user. UMA uniquely puts the individual at the center of the picture. It enables proactive sharing a la consent directives, reactive opt in consent and withdrawal and denial of consent any time; all with choice about the grain of sharing and all through a central location. The HEART effort is key because it uniquely focuses on patient centric, privacy sensitive health data sharing use cases, and because of its tightening both the security of OAuth, OpenID Connect and UMA, and their interop when applied to FHIR.

And some final remarks. The corporate practice of privacy has largely been about data protection and risk mitigation and the tools for solving consent problems have therefore been limited, understandably. However, pressure is now increasing to do more because of consumer skepticism, the regulatory landscape, growing data volumes and sources due to IoT and businesses need to demonstrate transparency so they can build trusted digital relationships.

In 2016, the API economy is no longer new and industry, agencies, patients and consumers are demanding more. UMA stands ready to form a key basis for these next-generation tools. Thanks very much for your kind attention and I look forward to any questions you may have.

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

Thank you, Eve and thank you to all of our panelists from panel one. We are now going to open it up to the task forces for questions. There are a couple of people already in the queue and a reminder to those who are not, if you want to use the hand-raising feature to put yourself in the queue, that would be appreciated. So our first question is from Josh Mandel.

**Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

All right. Thank you very much to all the panelists for this testimony and I would love to dig in with a question, this is applicable to many or all of the panelists who would like to share a perspective here. One of the things that we have been thinking a lot about in terms of healthcare data access are APIs that would allow healthcare consumers or patients to bring whatever Apps and tools they want to the table. In other words, this is a scenario where it's not necessarily the case that my doctor tells me what Apps use, but I might pick the one that I want and then try to connect that to my healthcare record.

So I'm interested in hearing from the panelists if they have exposed APIs in an environment like that where the clients are...the API clients are effectively brought in by consumers? And I know, for example, that Google through their developer portal allows me to register an App myself as a software developer and there are not a lot of steps that get in the way between when I register the App and when I can actually connect it to my own data. So I have been wondering if there are special considerations that go into supporting an ecosystem like that where you do not have a lot of control over what all the clients are or whether that is just the same kind of security considerations you would put in place in any API environment. And again, I would love to hear from any panelists who have thought about work in that kind of space.

### **Stephan Somogyi – Product Manager, Security and Privacy – Google**

This is Stephan Somogyi; since you explicitly mentioned Google, I figure I might as well pipe up. So from our perspective, it is one and the same. You know, what you just described is basically a web browser, you know, a web browser is something that connects to a remote server and what really matters is what the data is that is involved, how that data is appropriately protected, whether by technical means or by policy means. And I think that by and large, there is nothing particularly special from a technical perspective about how you protect that data. It is a very commonplace task today.

What makes this particular conversation, this context special is the nature of the data and there we have a mixture of regulatory compliance issues and just overall of sensitivity of the information. So that is where, in my opinion, things start getting a little bit higher risk, simply because of the stakes involved with the data that is being handled and potentially sent in both directions .

### **Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock**

Yeah, this is Eve. I would tend to break it down along business, legal and technical lines, so compliance. And there may be legal boundaries that are not compliance-related but business relationships and business opportunities and as well as technical security issues, for example. I mean...stuff may have gone down this route in terms of malicious clients of one sort or another. In my previous experience at PayPal where it was a financial, there were strict rules about the nature of clients that could onboard, so that had to do with the nature of the data or the nature of API access, the kinds of transactions that could be performed and the business risk that they posed.

### **David Ting – Co-Founder and Chief Technology Officer – Imprivata**

This is David Ting. So the issue, we often hear this concern about how patients can introduce their own data into the medical record system and in healthcare, I think the main thing that a provider or a healthcare organization worries about is the integrity of the data, whether the data is actually valid and whether it has been properly tied or associated with the correct patient; which means that you want to verify the identity of the patient and make sure that if the patient is actually producing this data, it is really for themselves and not some data that they brought in from someone else.

So you really want to be able to assert the integrity of that block of data from the moment the patient uploaded the data or introduced that into the system, tie that to a verified identity through some means. And in some cases, that identity may need to be a third-party validated identity, if there is any kind of medical or insurance costs associated with it. And the third piece is often consent around who can use that data, how may that data be distributed as well as ownership of that data and who actually has the right to modify and to distribute it.

### **Gregory Brail – Chief Architect – Apigee**

Hey, this is Greg Brail; I wanted to add one thing. There is one way in which APIs are different from web Apps in that an API gives the API provider an opportunity to authenticate the application that is accessing the data, as well as the end-user that is accessing the data. This comes to us from OAuth, which is one of the security technologies that are widely used in APIs that...

The advantage here is that this gives the organization providing the API, for instance a healthcare organization, the ability to set up policies about basically which developers are authorized to build applications that even access the API at all. Google makes good advantage of this, for instance, by setting up one authentication mechanism that ensures that only...the only way to get a Google login is via a web browser, but you also have to have an authenticated application. That means that you could

use things like use fraud detection techniques and other monitoring techniques that if an application does happen to sneak out through some unauthorized channel, that using an API in a way that may not be completely inconsistent with the terms of service, that application can then be shut down and its credentials can be revoked. So that is something that for instance when you...data via a Web App, you don't really have the opportunity to do, because anybody who can read the source code for the Web App on the browser can figure out various ways to get that...

**Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock**

Greg makes a great point here, you know, one of...it's maybe some serendipity that the way that OAuth was developed was to solve this password anti-pattern so that Alice the user didn't have to expose her real login to say Twitter, in order to have an application work with Twitter API on her behalf. But the result was that the client application has an identity and she has an identity separately and the security around the access to the API can leverage both those identities and apply security and fraud detection techniques over both of those at the same time as giving Alice some consent power, some authorization power over that application working on her behalf. It's a really pretty powerful set of capabilities which the rest of the technologies in that ecosystem can build on, and are.

**Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

So thank you all for those answers. I wonder if I might also call out or call on David Wollman for a perspective from the Green Button project. Is the notion of allowing consumers to bring their own Apps to the table to analyze their energy usage part of what Green Button offers out the gate or is it up to the individual energy companies to decide on that kind of policy?

**David Wollman, PhD – Deputy Director, Smart Grid and Cyber-Physical Systems Program Office – National Institute of Standards and Technology**

This is Dave, thank you. The situation being described is part of the use case that is covered by Green Button. You may think of that like the Apps should be authorized by the consumer so they can use the exposed API of the data custodian, with the App itself using the correct security and authorization credentials; that is one thing to add. And I will ask colleague, Marty Burns if he wants to add anything in addition.

One thing I would say is we have mentioned privacy already, I didn't get a chance to go into it in detail but one of the steps that we took in the Green Button system was to separate out the PII in the...from the actual energy users data streams; I know is going to be much harder in the health space, but it has created a much better situation working with privacy advocates and others to have a structural way to enforce PII restrictions. Marty, do you want to add to...okay, so thank you.

**Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

Sure, thank you Dave.

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

Thank you, Josh. Leslie Kelly Hall has a question.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Thanks, Michelle. Thank you everyone; this has been very, very interesting and I am heartened by your testimony. I think this creates great opportunity for patients and consumers. I have a question for both David and Eve. It seems to me one of the concerns that are raised about the opening of APIs is the fact

that EMRs, which are largely the group that holds our data, are...this is not a core competence and I agree with that. And I would like David to comment on the fact that by opening up the APIs, what this might mean to providing security modules that can fit in the ecosystem and to send our points of entry?

And then for Eve, it seems that with the use of UMA and combined with this, we have opportunities now to have much greater privacy control with time delineated usage, individuals being named. It seems between these two testimonies we have heard, we have, as I think Greg pointed out, opportunity for more security and more privacy. So if I could hear from both David and Eve about this premise is, have I leaped or is this possible?

**David Ting – Co-Founder and Chief Technology Officer – Imprivata**

This is...Do you want to go...which David were you looking for?

**David Wollman, PhD – Deputy Director, Smart Grid and Cyber-Physical Systems Program Office – National Institute of Standards and Technology**

Right.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Oh, I am sorry, Imprivata.

**David Ting – Co-Founder and Chief Technology Officer – Imprivata**

Okay.

**Arnold S. Epstein, PhD – Chief Architect – Imprivata 4410**

This is Army Epstein, I am the Chief Architect at Imprivata sitting here with David and I would say that, you know, opening up APIs to the EMRs, you can certainly put an API layer in front of the existing EMRs that may not have the full security profile that you would want because they were not built to do that. But I think it is a critical thing that we find a way to do that, to make that information available to applications that can enhance the access for providers and the various ways that providers can view patient information on behalf of treating the patients.

I also do think, and you know, hear from Eve as well that UMA or any other consent system is critically important for that so that the patient has a role in deciding who has access to what of their data. But I do believe that APIs, particularly FHIR as a straw first attempt at bringing data out for creative use is the future of how healthcare has to go; it can't be done by document, you know full document exchange like we are doing today.

**David Ting – Co-Founder and Chief Technology Officer – Imprivata**

This is David; now I just wanted to add one more point to that which is today with many of our EMR vendors, we interface directly via an API to them for electronic prescribing of controlled substances, where in order to conclude a transaction on behalf of the patient, a second factor authentication is done through our system so that there is not only the verification of the proper provider identity, there is also an indelible audit trail that links the transaction to an event in time to a specific individual. So EMR vendors will be...are very comfortable doing this provided there is a recourse to go after people who inappropriately use that interface or inappropriately use the system to compromise the privacy of the data.

**Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock**

Yeah, it's good stuff and so I guess I will follow on with that and say, you know, the opportunity is clearly there and one of the things that I have observed with the advent of FHIR has been, when you put something into the terms of a RESTful API, the first thing you are able to do with it is have a hack-a-thon, and people have and, you know, there is a server you can play with now, and there is movement that you can see directly and it's actually an exciting time for that reason. I mean, RESTful web based APIs can make things happen.

And that is why I made my remarks about the IoT economy, essentially. People of been doing embedded programming for a long, long time, you know, 15 years at least but the reason we have an IoT economy is because you can take people who can do web based, web style programming and apply it to physical devices in the real world, and we're having a revolution actually in clinical and consumer health devices because of it; so it is kind of exciting for that reason. I mean, things can improve quickly that way.

And so what I am finding is that the conversations that I am having around user managed access and its implementations, including things like MITREid Connect and my own companies Open Source Project are because the data volumes and the data sources are increasing because of that, and a lot of other reasons but partly because of that. And just like OAuth was born because we really needed a standardized answer to the anti-password problem, we didn't want to be sharing our primary credentials with services that shouldn't have it.

This new pressure of data is causing us to need that because hey, if you have SmartFox, which there is a company near me in Seattle that makes them, you know, dumb socks are there when you don't need data generated by your socks, but smart socks is there when you do need data generated, and you don't necessarily want to share that data with just with yourself using a client App, you want to share it with somebody else.

And now we have the password anti-pattern, I'm sorry; I was misnaming it before, with sharing it with another party with whom you don't share credentials at all. So you need to share with another party that you don't have a login shared with. So we kind of did the share button for data and it would be nice to have it in a standardized basis because the data streams in our lives don't actually have boundaries the way we think of them, a health vertical, a consumer vertical, and smart home vertical and so on; so, it is going to be the case. Yeah.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

This is just Leslie in follow-up. So what I am really hearing is that the advent of the APIs and the use in healthcare give us opportunity for more security and more privacy and more flexibility and these things are not mutually exclusive.

**Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock**

Absolutely and I think it's because we found...because APIs came into play as I like to say, for fun and profit; they had business motives, you know, APIs have project managers now, some do. That the security solutions, so to say, that, you know, API management platforms came into play like Apigee, that we have a robust solutions that do take that approach that it's a defense and depth, because it has to be defense and depth because we put our API endpoints on the edge of the network. And we do have that opportunity to actually have a no compromises solution if we do it right, applying the lessons that we have heard from Google today in the testimony, which I think were really good, good advice.

**David Wollman, PhD – Deputy Director, Smart Grid and Cyber-Physical Systems Program Office – National Institute of Standards and Technology**

And this is Dave Wollman; one additional point to make is that, if you are interested in assuring privacy, you also have the notions of scope negotiation and granular access permission that can help provide the infrastructure where you can do a better job of managing the privacy.

**Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock**

Yes, when I was talking about fine-grained that's exactly what I meant, you know, if you can set policy for access by somebody else and then go away and not be there when they attempt access and then be able to say withdraw your consent later on or withdraw some consent, basically say I don't grant you that scope anymore, that is at least scope-grained access control by an individual.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Thank you. Thank you very much.

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

It looks like Josh Mandel has another question.

**Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

I do; so this was a question in response to Stephan's comments about an engineering culture, and it seemed like this was, in some sense, the most critical issue when it comes to building an API that is not just secure, but that evolves over time and continues to track and drive best practices in security and in privacy. At the same time, fostering this kind of culture is a soft science and it requires a tremendous amount of organizational buy-in.

And from my perspective, when we are thinking about the right that a healthcare consumer has, the right that a patient has to access healthcare data, and sometimes that right is invoked against the direct interest of the hospital or provider organization that "has the data." So the organization that would need to expose these data on a patient's behalf doesn't always have the deepest kind of buy-in, and sometimes the only reason they are exposing it is because they are regulatorily obligated to expose it.

And so for me that's a conundrum because on the one hand do you want to support this kind of engineering culture, but on the other hand maybe there is motivation for exposing those APIs doesn't really come from that deep down. And so that's for me, a difficult and big question and I wonder if any of the panelists have thoughts on how you can promote that kind of engineering culture, especially in an environment where the ones exposing the data and hosting these APIs may not be deeply intrinsically driven to do so?

**Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock**

That is the bacon in the sandwich isn't it? I am pretty sure the transcriptionist may not have ever typed that before. Yeah, that is a business model challenge and that is where it gets interesting because a lot of the, let's take IoT again as an example. Consumer IoT devices exist to generate that data on behalf of the consumer that buys them generally, so they have the motivation to do what the user wants with the data. And that isn't the case necessarily given, you know, the business model realities of, you know, many parts of the healthcare system. And oftentimes regulatory compliance is what sort of turns the crank in that case, and that is sort of an unpleasant way to change things and I don't necessarily advocate that but data comes from a lot of sources; that is the reality in everybody's life. I mean, if you

have a connected car or if you have a Cloud file system or if you have whatever it is your data actually does come from many sources.

If some of the data starts to be stuck where it is, it could be that consumer pressure on those sources actually does work at the margin. Or if it doesn't, then it is stuck and then we are talking some species of data blocking; it is a lack of data portability if regulatory pressures doesn't actually come to play. That's not about engineering culture; that is not about API design at all, that's about business model.

**David Ting – Co-Founder and Chief Technology Officer – Imprivata**

Yeah, but I think that the challenge there is actually was brought up by the other David when one of the roles he talked about was data custodian. And what really needs to be clarified in healthcare is, is the patient's health record, procedures and so on that have happened at a provider, is the provider the owner of that data or the custodian of that data on behalf of the patient?

In general I believe that doctors want to be able to access data about patients outside of their own hospital when they are trying to treat a patient to get a better view. And so on the patient's behalf, we should all be in the place where that data should be freely available and the biggest challenge is the identification of the patient and make sure you are giving the records of the right patient. But I think that the clarity of who owns that data and who can do what with it needs to be stronger in the ongoing conversation.

**David Wollman, PhD – Deputy Director, Smart Grid and Cyber-Physical Systems Program Office – National Institute of Standards and Technology**

This is Dave Wollman and can I respond to that? We have learned something from the energy space in that it was difficult to get into data ownership questions; it was easier to look at access capabilities by consumers to their own data recognizing that utilities will always need access to the data for operational purposes.

And speaking to the culture part, it was a culture change to work with utilities which have very closely protected privacy and to get them comfortable in sharing and in the end it was kind of the efficiencies and the ability to use a national standard in doing so. They had been working like with spreadsheets, etcetera; this gave them something to latch onto that was more common and they are able to advance that. But, they were taking privacy very seriously, but the whole issue of the access to the data was a better vector for us to go down than ownership.

**Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock**

I would love to talk to you off-line about that because I have been developing some elements of consent strategy where a company could have consent vulnerabilities in the sense that the business could have, a business could have usability vulnerabilities in addition to security vulnerabilities when they develop say an authentication strategy. Because people get sensitive, as we saw when Spotify deployed a new terms of service and everybody freaked out seeing the wording and maybe it wasn't marketed well or written well or maybe it really was pernicious. But there are ways to do these things well and there are ways to explain to people what is necessary for an organization to function and where it is appropriate, to ask people for consent to share.

**Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

Thank you.

**Alisoun Moore, MPA, MBA – Senior Director of Corporate Development for the Federal Sector – LexisNexis, Inc.**

This is Alisoun Moore from Lexis; I know I am on panel two, but would like to comment. I believe providers own the data but patients arbitrate for their own data via the HIPAA law. So patients are...to give consent to providers of whom providers can share that information. And there are many different parties that providers share the information; they are sharing with insurance companies. They are sharing with other specialists and then most providers when you go in and you sign the privacy form, they have written in there that they have an ability to share data that is in the patient's best interest while treating the patient and only if the patient changes that form would it restrict what the providers...who the providers can share their data with.

It gets a little cumbersome. I love the BLT sandwich, I think that's great, it gets cumbersome if you are allowing patients to write their own APIs or develop their own Apps because they could possibly compromise some of the regulatory restraints that either business associates or providers themselves have with respect to privacy and the HIPAA law specifically.

**Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock**

This is why I almost hate to talk about data ownership and why often in legal circles they like to talk about property ownership as a bundle of sticks because it's just about what rights you control and it is why, even though UMA is stuck with the OAuth terminology around resource owner, it really just means, do you have the rights to control access to this resource? It just clarifies things if you talk about control; control which aspect of the digital resource? So I am sensitive to what you are saying for sure.

**Alisoun Moore, MPA, MBA – Senior Director of Corporate Development for the Federal Sector – LexisNexis, Inc.**

And unfortunately when HIPAA first came out and actually probably for the first decade it was out, the law was used to restrict access in many cases, rather than what the law was intended which was to open access in a secure way so that electronic exchange could indeed take place.

So you have this big cultural issue that had to be contended with and then you have the advent of the HITECH legislation coming in and requiring the Meaningful Use and adoption of EHR records; that actually, I think, has opened up a lot of access for patients if only on a patient to provider alone and not patient to provider then provider to provider, provider to all of the patient records, which as we know, can reside in multiple provider places let alone the business associate and employer data, that employers who are self-insured are at least privy to on a de-identified basis.

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

This is Michelle; we have a number of people in the queue so we want to make sure we get to all of our questions. Aaron Miri?

**Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center**

Yes, thank you. First of all, thank you very much to all of the panelists, excellent job, excellent testimony. My question would be coming from the perspective of a provider hospital; I am a CIO here at a hospital in Dallas, Texas so take my question from that lens, please.

Specifically I would like to ask a question of both Google and of Imprivata; this is going to be regarding data provenance. So my question specific to Google, as respective application APIs that you have were

exposed to the public, and thus application and respective databases began to resend and receive data via those APIs, have you had any difficulty in maintaining quality aspect of that data? Have you found any need to scrub or filter that data or are the APIs so well documented and published that they are strong enough in their format and this is a nonissue?

My second question is specific for Imprivata; you mentioned, David, given your success in working with various EMR vendors, and as we all know, EMR vendors predominantly are very closed-loop systems and are somewhat limited and restricted on what data they share, so therefore Imprivata is blazing the trail here.

I am wondering if you can educate the committee on any needs or any items you have found around standards development for data citation with regards to APIs. Are there any special heuristics? Are there any context information that is particular to healthcare that the committee needs to pay attention to, so therefore we know that an API is establishing that trust and it is facilitating a trusted data transaction? I am really curious, especially since you talked about e-Prescribing; so both Google and Imprivata, if you could answer please.

**Stephan Somogyi – Product Manager, Security and Privacy – Google**

This is Stephan from Google; I guess since I caught the first question, I will respond initially. From our perspective, APIs and data quality are not really that related. The API is a facility to allow access, allow appropriate access to data, but the actual data itself should largely be disconnected. Sure you have to package it in a form that is useful for the purposes of transmission, for the purposes of interaction between the back end systems and the client side systems; but there is nothing inherently about APIs that really have a significant influence on the data quality. All of the controls that you need to put in place, all of the policies and process and in many ways also ideals that you have to put in place to make sure that the data quality remains high are, as I say, they are orthogonal to the API issue at hand.

**Arnold S. Epstein, PhD – Chief Architect – Imprivata**

Yeah, and this is Army at Imprivata. In order to answer our second question, I think that it is what we do with the transactional work we are doing with the EMRs now is to capture...to make sure that the transactions are well documented, that the source system from which the data is coming, the person who is making the request, the subject of that data has all have to be well identified. And the permission from that subject has to be documented as well and of course the time of the transaction as well. So along with the data, there is a set of metadata that allows you to audit and know that pol...and review that policy is being followed throughout the course of business.

**Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

Okay good deal, so I basically to summar...and thank you both for that. So basically to summarize, kind of just for layman's sake here, so from Google's perspective, the API is basically a construct to allow, so think of it as a tunnel on the highway basically. You go through the tunnel and that's what it is, built to a certain standard.

From Imprivata's perspective on teaching us something, given a set of standards, now I am driving through that tunnel, I am going a certain speed limit, I know what color car I am in and whatnot; as long as that is all up front, trust is established. So now you have a construct that is a trusted construct that data can travel through that is well documented.

So from a quality and data provenance perspective, and as it relates back, as I am a provider hospital, giving that information back to say, some sort of regulatory agency, all of that will be available and facilitated, therefore establishing trusted transactions. Is that correct?

**Arnold S. Epstein, PhD – Chief Architect – Imprivata**

Yeah, you got it.

**Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

Perfect, thank you.

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

Meg Marshall?

**Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation**

Hi, yeah, thanks. So first of all, thank you to everyone for the presentations and great conversation. My question is directed toward Stephan at Google. You discussed during your presentation that Google uses and leverages best practices for the protection of data. And I guess that this is a high-level question but I am curious if you could describe those best practices for us. Are these specific to Google? Are they industry standard engineering practices and how do you support innovations in those best practices that keep up with advancements in technology?

**Stephan Somogyi – Product Manager, Security and Privacy – Google**

This is Stephan. Unfortunately to provide a comprehensive answer to your question, we would be here for at least a couple more days to come, so I will try and be relatively concise and hopefully won't succumb to the temptation of terseness.

I think at a highest level you have to keep your eye on the forward march of technology. And let me in fact scope my response down to security and let's take an easy and concrete example in the form of encryption. By and large, Google makes a great deal of effort to assess the risks related to encryption, particularly around unauthorized data disclosure and where we feel existing practices have become outmoded. We tend to be fairly robust in deprecating older standards.

We have a very applicable situation going on right now where Google as well as all the other major browser developers, we are in the process of no longer allowing a certain cryptographic cipher, RC4 to be accepted by browsers anymore. This used to be a perfectly reasonable best practice kind of thing, but over the years, technology has moved on, computational power has grown, and we are now at a point where we now know that RC4 which once was an entirely acceptable practice, is now, in fact, a worst practice. And so as to make it as straightforward as possible, we are taking the active step of not merely letting it wither on the vine, but we are actively going to start disallowing it.

Now that is a really scary sort of thing for a lot of organizations to do because they have legacy systems that they need to keep up and running, from a budgetary perspective they have to allocate the necessary resources to do the necessary update or deprecation. So taking the approach that we do brings a lot of work with it but ultimately our paramount concern is protection of our users and their data. And so if we are aware of a situation where a given risk mitigation avoidance is no longer fit to do exactly what we need it to do, we will quite aggressively get rid of it and we will accept that this is part of the cost of doing right by the user.

And yes it is going to be somewhat inconvenient for some, but ultimately again the primary motivator here is user data protection and that actually loops around to the question from the gentleman earlier about the engineering culture. It is not just a matter of buy-in, but it is also a broader and deeper commitment to saying that the most important thing is to do right by the user and the rest will follow.

**Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation**

Thank you very, very much.

**Stephan Somogyi – Product Manager, Security and Privacy – Google**

I hope that adequately answers the question.

**Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation**

That is very helpful; if I could ask a follow on to that; what is the disruption to the consumer as far as the notification or the education that this is happening? And I realize that this is a very complicated process but just again, kind of keeping at a high-level, is this something that the consumer then becomes aware of and they understand and could perhaps contact their technology, for example, if it is something that they want to see continue?

**Stephan Somogyi – Product Manager, Security and Privacy – Google**

If everybody does their job right the user should never notice. We are neither capricious about these types of deprecations nor do we do them on short notice. To take this very concrete example again, we have been talking for some time and not just we, but also other browser developers, have very much in unison and very harmoniously have been singing very, very loudly that this is going to happen.

Now unfortunately, not everybody paid attention and so there are systems still out there today that absolutely require some of these older, less secure mechanisms in place. And the user is going to run headlong into these systems at which point the browser will probably tell them, I cannot connect securely to this thing that you are trying to connect to; there is a problem. Unfortunately at that point there is no real, human-friendly way of communicating the technical minutia of what exactly is going on.

But what the service provider that hasn't kept their systems up to date is going to notice very quickly is that whatever mechanisms they have for customer support or to gauge customer satisfaction, that is definitely going to start moving the needle because they are going to be getting a lot of phone calls saying, you know my current browser cannot connect to your thing, but I need to connect to thing to get my work done; what is going on?

And at that point, the service provider is already very much behind the ball and then they essentially have to take a process that could have been managed very carefully, foresightfully, and with reasonable speed and turn it into a fire drill. And that is unfortunate and that benefits no one.

**Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation**

Thank you.

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

Sorry; Josh Mandel?

**Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

Thanks. So we heard from a few of the panelists about consent models and the kinds of permissions that users are able to get when in time they are able to give permission, what are the exact scopes of permission they can grant? For whom does the permission apply? And I'm wondering if those in the panel who have deployed OAuth-based solutions can speak to their experience using OAuth in order to allow this kind of consent and what are the parts that have gone well and whether have been challenges in exposing either fine-grained consent or other aspects of what you might want in terms of expressing the depth of the user's choices? So some real-world sort of experience, does OAuth cut it? Or where are the places that it might break down?

**Gregory Brail – Chief Architect – Apigee**

This is Greg, I'll just start with a short little bit. We, you know, OAuth is part of our product and many of our customers use OAuth as a way to provide authorization on API calls. And OAuth is very effective because it is so flexible. For instance, the end-user can be authenticated using a web browser, using a SAML token, using OpenID Connect, using Google authentication, whatever. And then we have a lot of control over the token.

OAuth includes a very simple authorization granular model known as the scope. So in simplistic terms, for instance an application can be allowed to have read scope and write scope, but not, you know, super-user scope. And particular end-user may ask for certain scopes and they may be granted a subset of scopes. And for simple use cases, OAuth, this scope mechanism is a very effective way to communicate to developers in a very simple way, you know, you can build an application that can read the database but can't write to the database.

I think there is a level beyond that at which we get to a more application-specific style of authorization. You know, is the user authorized to view patient records for patients from another hospital after 10 PM? Where I think the very simple scope-based model of OAuth authorization is not sufficient and you need to look at solutions that are a little bit more complex and full featured; so a combination of some kind just makes sense.

**David Wollman, PhD – Deputy Director, Smart Grid and Cyber-Physical Systems Program Office – National Institute of Standards and Technology**

And this is Dave Wollman; if the organizers could un-mute my colleague, Marty Burns he would like to contribute here because this question on scope negotiation is relevant to our Green Button experience. Marty are you able to speak?

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

We will have to work with the operator to move him over, so, we will try and do that now.

**David Wollman, PhD – Deputy Director, Smart Grid and Cyber-Physical Systems Program Office – National Institute of Standards and Technology**

Okay.

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

They are live now.

**Martin Burns, PhD – Smart Grid and Cyber-Physical Systems Program Office – National Institute of Standards and Technology**

Okay thanks; hi. So yeah, scope negotiation is a really big part of Green Button and we made use of the OAuth scope capability. But what we do in Green Button is prior to the authorization phase, when the customer logs in to I guess what you call an EMR, the customer will be interviewed for what he wants to authorize for a particular third-party or third-party application and a scope string is computed from those responses. That scope string has no PII, no identifiable information; it is just a string of options that are agreed to. And it is important to us that during this scope negotiation that the scope be acceptable to all three parties.

So it may be that in the case of the holder of the data, there is certain data that they might want to be able to provide to a third-party on behalf of the customer; but that might be the data that the third-party really can use. So what happens is during this scope negotiation, we use the same redirection methods that OAuth2 uses and when forwarded from the data custodian, we call it the data custodian site to the third-party, the scope options are provided to the third-party who can either accept them and start the authorization sequence with that scope or he can redirect the customer back to the data custodian accordingly to approve what the third-party really needs.

Once that whole thing is established, using the scope strength from the OAuth2, then the authorization occurs and an access token that represents the granular rights to data, not wholesale, but the granular rights to data agreed to. And after that if the retail customer wants to modify the scope, he can do that at the data custodian and we have a notification method by which the third-party is notified that a change has been made. So, that is sort of how we dealt with this challenge and I think we have successfully done that.

**Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

I would love to hear from other panelists as well, but just to push a little farther on that experience; can you speak to how this has gone in the real world? Do you know whether consumers of energy data have been able to grab these scopes and understand what they were granting? And whether they were able to express the kinds of permissions they wanted using this model? Or did some users struggle and say, I couldn't figure out how to share what I wanted without sharing too much? What has the real world deployment experience been like?

**Martin Burns, PhD – Smart Grid and Cyber-Physical Systems Program Office – National Institute of Standards and Technology**

Honestly it is too soon to tell, but basically they don't get presented with all the choices, they get presented with dialogues from the holder of the data for the kinds of choices that they really want to make and then, you know, a simple GUI that is not standardized is used and then the scope itself is encoded behind the scenes.

**Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

Thank you. And I would love to hear from others who have deployed OAuth services about what those experiences have been like, you know, especially when it comes to users either not being able to express some of the things they might want to or conversely, in a model where you think you have been able to help users share at the right level.

**M**

When you say users, do you mean people who use applications that use APIs or do you mean people who build applications?

**Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

Ahh, so I mean people who use applications that use APIs that authorized using OAuth, and then in particular the sort of negotiation steps where a user can say, these are the permissions that I want to share or not share with its App...but, I authorize it.

**M**

Resource owners, roughly.

**Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

Yeah.

**Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation**

So Josh, this is Meg and if you don't mind, I could maybe add a scenario; that was one of my questions that I have been thinking about how to ask. In the healthcare world, two really good examples I think; one is HITECH provides patients the right to restrict access to payers any data related encounters which they chose to pay cash for, for example. So if I am negotiating the scope of data that I want sent to an App for my insurance carrier, for Aetna or whomever, how would that potentially work? And I think the comment earlier, I don't remember who made it, that a consumer can destroy the regulation protection that are provided to them; I think is really interesting in this whole negotiation point as well.

And just one more example of where this could potentially come into play is around the 42-CFR Part 2 data where the type of data is restricted based on the type of provider who captured it, and there are all sorts of different requirements that need to be attached to the data moving forward.

So Josh, I think this is a really great question and really gets to the heart of, you know, some of the specifics around trying to negotiate that consent that has been so carefully guarded and protected within the EHR that is now at the request of the consumer, but other parties will have access to that based on the consumer's request. So thanks for the question and I hope I didn't confuse that too much, I just wanted to provide a couple of examples.

**Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock**

This is Eve, if I can actually give an example that I consider an analogy that has animated a lot of the UMA work and perhaps it looks a little bit like OAuth under the covers, I don't know. And it feels a little weird with Stephan here giving it but, the example is actually Google Docs and many of the Google Apps because many of the interfaces that we have been building in our UMA implementation where I am look like a share button. So some of the use cases for using UMA look like proactive sharing or delegation.

And the idea of scopes would be that hey, if you want to share view access versus edit access you can. But if the default is to just unthinkingly share all of the scopes, what you typically would want to do, or if the use cases you are asked to share data and you unthinkingly share all of the data, then most of a typical person's experiences, needing to go back when something went wrong or you have a question or you just have the opportunity to monitor what access was shared and you want to change things to scope them down, then you do that.

And so I have had many an occasion to unthinkingly grant edit access to a bunch of docs, to a bunch of people, and then I go back and realize something went wrong and I change it to suggest or view or whatever it is, and I am glad I did. So the proposition with UMA is, any API designs whatever scopes are appropriate for whatever the resource sets are sensitive, and you do have to think about scope design, and I think in the modern API world, scope design gets more and more critical and you can go into that if you want to, but many is the time that I want to later withdraw selectively the permissions that I handed out; not now, but later.

Now I want to be expansive because I don't have the time, later on I want to think more strongly about that and kill access for some people and limit access for others, people or parties or whatever they are. So that sort of vision has animated a lot of the UMA work and it is something that I actually do, maybe not on a daily basis but probably at least on a monthly basis. And having a central place to actually be able to do that is even more valuable than being able to do that on an application by application or resource by resource basis.

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

Any other comments from our panelists?

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

It's Aaron; I have one quick question.

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

Is this Aaron Seib?

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

Aaron Seib, yes ma'am.

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

Go ahead, Aaron.

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

Well it was just, you know, mentioning scopes, it is really helpful, it helps clarify why, you know, moving to APIs helps improve the equation of making access easier. Eve, you mentioned this BLT formula; business, legal and technical. It seems as we improve say scopes and other methods of controlling granular access, does the business and legal requirements ever go to zero? Or do we always need to anticipate that there is a business component, there is a legal component; can the technology eliminate those other two components?

**Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock**

In my opinion, no. There are some things that can be amenable to technological treatment like security solutions, you know, there are technological solutions that more and more can handle things that we did not think they could before. But it is always an arms race; Stephan has been eloquent about how you have to move forward and not assume that solutions that worked before will work in the future.

But, you know, building relationships even with business partners is something that, we are always looking for dynamic onboarding of partners and client applications and so on and I think it is a really good thing to strive for in how we build our technical solutions to allow for dynamism. Oftentimes even if you allow for that and build for that, and I think we should never preclude that possibility, the way businesses tend to operate is to not like dynamism; they like static partnerships to be built because businesses, just like people, like trust and it takes time to build trust.

So even if it is possible to develop technical trust quickly, developing business trust takes some time and it often involves contracts. And I had mentioned in my oral testimony that there are solutions coming along for...involving legal agreements, but I still think that those will tend to take time. The one I was thinking of is called Common Accord and it is very, very interesting and I think it can squeeze some friction out of developing and making legal agreements. Nonetheless, I think “B” and “L” will always exist. That’s my opinion.

**Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center**

And this is Aaron Miri, I am a committee member and I am, again, as a CIO of a hospital, I want to echo what Eve just said; that is as top of mind in risk appetite, risk management, I mean, there is zero that we leave to chance or speculation. Everything is very clearly documented, especially when it comes to data and when it comes to anything around the privacy and security domain. I mean, given how heavily regulated healthcare is, especially of a hospital system, I cannot risk anything to chance. So while technology may allow for better risk appetite, it will never mitigate it to the point of zero, in my personal opinion as a CIO. So I echo what you just said.

**Eve Maler – Vice President Innovation & Emerging Technology – ForgeRock**

Yes, careful balance.

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

Other thoughts?

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

This is Leslie and I, another panel mem...not, another committee member rather and I just had a comment because what was earlier said about having the patient give away all their rights by making information available, they are not giving away their rights; they are exercising their rights. They have the right to have it as private as they choose or as public as they choose. I think the obligation becomes how do we educate so that people understand their risk, but ultimately it is the patient's right to choose. So I just wanted to comment on that because I hear us thinking somehow there is a higher risk when the patient chooses to use their data as they wish.

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

Amen.

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

This is Michelle; it doesn't look like we have any more questions in the queue, so I will turn it over to the task force to see if there are any more questions before we move on to our next panel. Umm, okay, hearing none...

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

Can I ask one question, I'm sorry Michelle?

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

Yes, go ahead.

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

I think it was Stephan, he mentioned that there is a presentation; one of his colleagues is giving in a couple of weeks, a deep dive. I would love to learn more about that if I he gets a chance to share that with the task force.

**Stephan Somogyi – Product Manager, Security and Privacy – Google**

Absolutely, I will find a way to get those materials to you in some way. I don't know exactly what the time is when it is being presented but yes, we will see what we can do and we will follow-up.

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

Thanks, appreciate it, it is worthwhile.

**Stephan Somogyi – Product Manager, Security and Privacy – Google**

Thank you for your interest.

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

Thank you. So thank you again to our presenters on a panel one. We are running a little bit early, so I just want to make sure that we have all of our panelists available for panel two and we will just rearrange if need be. Alisoun Moore, I believe you spoke up earlier so I think you are on.

**Alisoun Moore, MPA, MBA – Senior Director of Corporate Development for the Federal Sector – LexisNexis, Inc.**

Yes.

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

Evan Cooke?

**Evan Cooke, MS, PhD – US Digital Service at the White House**

Yes, I am on.

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

Hi, Evan. David Berlind?

**David Berlind – Editor-in-Chief – ProgrammableWeb**

Here.

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

Hi, David. Marc, you said your last name earlier, I should have caught it; Chanliau?

**Marc Chanliau – Director, Product Management – Oracle**

Chanliau.

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

Can you say it again? Chanliau, okay.

**Marc Chanliau – Director, Product Management – Oracle**

Chanliau, yeah.

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

I am just not going to say it and butcher it. Gary Brooks; I'm sorry, Gray Brooks? And Shue-Jane Thompson from IBM?

**Shue-Jane Thompson, DPSM, ITIL Expert, PMP – Partner, Cyber and Biometrics Service Line – IBM Public Sector**

I am here.

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

So I think the only person I did not hear was Gray Brooke, so we will just have him go last and hopefully by the time we get there, he will be on. So Alisoun, if you are ready.

**Alisoun Moore, MPA, MBA – Senior Director of Corporate Development for the Federal Sector – LexisNexis, Inc.**

Yes, I am; thank you very much. First I want to thank the committee and the API Task Force for the opportunity to provide comment.

LexisNexis Risk provides risk mitigation services and data to many industries, including healthcare. We do this by assimilating information from over 10,000 public record sources to determine correct identities of individuals, businesses and healthcare providers. We then use this information for thousands of businesses in banking, insurance, real estate, government, law enforcement, healthcare, payers, providers and many others to ensure that the transactions that they are conducting are done securely and that they protect consumers.

In the course of this business model, we routinely offer secure real-time and secure batch processing of customer data which is run against our data to verify the information that is provided to these businesses. We do allow APIs, but with very strict controls and safeguards for clients who need to access their sensitive data and also to protect their sensitive data.

We take security and access control very seriously with both sets of data. We audit and monitor employees, our own employees, and we provide a very thorough credentialing process for our customers before we provide access to our data. And this is just a quick synopsis of the security and

policy controls in place...that we have in place, so that only authorized people can access the information that we have. Customer access is then monitored and audited; yes we do actually audit our customers, as well as abide by the government regulations for specific data usage agreements in place to ensure appropriate and proper use.

So in summation of just my opening comments it is, we are under lot of regulation as a consumer information provider and we take that very seriously. And we have put in the appropriate safeguards to allow that to occur; and our customers expect that from us. So why don't I just go through the questions and answer those each directly.

So the first one is, does our organization use APIs for Apps which are available internally or third-party? Yes we do, but with strict usage and access policies in place to protect all parties.

Do we publish our documentation online and make it available to third-party developers? Yes, our customers are provided access to the documentation, once they have been credentialed and appropriate non-disclosure agreements signed. All clients who wish to procure access to our data must follow internal processes for technical integration, but also must conform to data usage agreements that protect their data and guide their use of our data as they use it.

All clients must abide by pertinent federal and state laws, such as FCRA and HIPAA that we discussed previously. We...it is important to note we are not a software firm, so we don't normally develop APIs for commercial use; what we do is we have developed APIs to link directly to our clients and serve their specific needs and we have business requirements before on how we construct those APIs and how we transfer and allow access to our data.

So how do you get, excuse me, how do you determine who could get access to our APIs is based upon the client-specific needs and what specific data they have authorization to access. We don't allow open access for just anybody; it is usually done by what their need is. If they are law enforcement or if they are a healthcare provider, they have to actually fill out what the need is and conform to the laws thereof.

We are a data services company and we are regulated by federal and state statutes therefore we work very closely with our clients to ensure they understand how they can use our data. For instance, we have a product called Tri-Header which is where we merge the three credit reports into one report; there is only one permissible use for that and that is for employment checks, and so that is just an example of what I mean when I talk about clients access and permissible use.

And then when we have agreements with our clients and licenses signed, we set up secure access using secure web services and secure file transport...protocols integrate those systems. And some of those are directly into our systems, for instance the property and casualty insurance market where we have about 100% participation; they access our hosted data set, but that hosted data set is almost always connected directly to their internal systems so than in a driver goes in and applies for insurance, the customer rep can pull up their entire driver file and any claims history that they have from whatever insurance carrier they previously had insurance from, right then and there in just a few seconds time to be able to quickly underwrite that driver and provide them insurance as quickly as possible.

Do they need to be certified for privacy or security standards by our organizations to use? Yes. As I have been mentioning, we have a credentialing process for all customers and partners who access sensitive

LexisNexis data. This could include a site visit to the customer or partner's facility as well as data use agreements and usage policies, including monitoring and audits to ensure compliance with our privacy, security and data usage agreements.

I will mention here that this is equally important for our clients, in the data usage agreements that we sign with our clients, they are also asking us to abide by their policies and letting...and assuring that we will not share their data with anybody outside of that data usage agreement. So that DUA is an absolutely critical document for both parties to have.

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

If you could wrap up Alisoun?

**Alisoun Moore, MPA, MBA – Senior Director of Corporate Development for the Federal Sector – LexisNexis, Inc.**

Pardon?

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

If you could please wrap up.

**Alisoun Moore, MPA, MBA – Senior Director of Corporate Development for the Federal Sector – LexisNexis, Inc.**

Yes I can. So other terms that...terms of usage could include specific language for privacy and security; yes, again we have very specific requirements for privacy and security. Are there production deployments of these APIs and third-party applications? Yes. We do have production deployments but again, they are specific to our clients.

And, what are the perceived and actual privacy and security concerns or barriers of adoption to the APIs? Like any technology, if the APIs are not developed or governed with strict security controls and data usage policies, security and privacy will be compromised. And I think the panel previous to this had a lot of discussion about that, it's that BLT sandwich and "B" and "L" are the sort of governance of the API. And so the "B" and the "L" and the technology must be carefully planned out and developed.

And then how do you improve customer experience for third-party Apps using APIs? Just from my experience as a former of public sector CIO and assuming you have accomplished the security and policy and technology hurdles, the technology has to be very seamless and useful. Use of focus groups to achieve this, development of intuitive user interface and very fast response times are key to adoption by consumers.

And then the last question quickly is are there third-party certified authorities in non-healthcare industries that we can leverage? And I was not aware of any, so I will wrap up that point. Thank you.

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

Thank you. Evan Cooke?

**Evan Cooke, MS, PhD – US Digital Service at the White House**

Thank you. Thank you to the task force and panel for the opportunity to participate today. It is a real honor to be here on behalf of the US Digital Service at the White House to support the application of modern API technology to improve healthcare outcomes for our nation.

Prior to joining USDS and tour of duty from the private sector, I was Co-Founder and Chief Technology Officer at Twilio, a cloud API platform for building communications applications that today serves more than 700,000 API developers. I would like to start by emphasizing the incredible power of APIs.

The Department of Education recently launched the College Scorecard application built on top of an open API with data from 7000 colleges and universities going back 18 years. This API makes it easier for software developers and researchers to extract, customize and build upon the data to support students and families to help them make the college choices. The result has been a diverse ecosystem of partners that support better college search and choice tools, better advising and support for students and more comprehensive rankings with new outcomes data. This is just the beginning of what is possible and it gets me incredibly excited.

The idea I would like to explore my comment today is the notion of APIs as a collection of technologies and standards rather than as monoliths. As we look to the future of APIs in healthcare and how to promote security, privacy, innovation and interoperability, it is helpful to consider a fine-grained approach.

A common way to describe APIs is as software contracts between parties; those parties could be private companies, individuals or public entities like federal, state or local government. APIs can capture almost any form of business process or exchange of information if the data can be represented appropriately in digital form that can be exchanged over a network.

I will start by sharing a brief story from my previous experience in the private sector. Years ago, when we started Twilio, we were able to implement our own REST API with tailored security mechanisms and data formats. During the first few years, the API changed quickly and the ability to make and deploy changes was critical for meeting customer needs providing better scalability and reliability and improving security.

While some parts of the API did change quickly, other pieces such as the serialization format and the data like WAV or MP3 audio formats, did not change. So rather than a single entity, APIs are composed of many parts such as network protocol, security mechanisms and transports, authentication and authorization means, request response methods, and serialization formats, those parts may need to change at different rates depending upon their maturity and broader changes in the products that those APIs support. Thus as we think about APIs and the processes for standardization and certification, it may be helpful to think through each component separately, as appropriate.

Because the requirements of each API can be different, the specificity of guidance may also need to be adjusted depending upon what component of the API is being referenced. For example, we might decide to dictate a specific technical format for a mature serialization format, but provide higher-level guiding principles rather than technical specifications for a request response approach. ‘

As an illustration of the possible levels of abstraction, consider the NIST, National Institute of Standards and Technology Cybersecurity Framework that describes four different levels of specificity; that is,

function, categories, subcategories, and informative references. The implication of this more fine-grained approach to APIs is that a uniform technical specification of an API and a corresponding certification of that specification may be difficult.

One approach would be to standardize or certify parts of an API together or independently. Another approach and one commonly used by private sector cloud providers supplying resources like storage, compute or workloads as services, is to certify the organization providing the service. That approach would focus on the provider of an API rather than on the technical protocol.

There are, of course, a lot of questions about building trust with API providers and with the data provided by those APIs. But I would like to conclude by reiterating my excitement for the potential of APIs and to advocate for the notion of APIs as a collection of separate functions and technologies that may need to change at different rates and may require different levels of specificity and guidance.

Thank you for the opportunity to participate today and I very much look forward to the discussion.

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

Thank you, Evan. David Berlind?

**David Berlind – Editor-in-Chief – ProgrammableWeb**

Yes, thank you to the task force for the honor of being asked to testify in this matter. For more than two years, ever since an API-related attack impacted thousands of Twitter and Facebook users, I have been researching API security from a real-world perspective.

Every time there is news of some major exploit, such as a major retailer getting compromised, I go through this list of questions. One, was an API involved? If so, two, what was the final objective of the hackers? Three, what role did an API play in achieving that objective? Four, did the API provider leave its guard down or did the hackers rely on a new or unaddressed vulnerability in standard API technology. Or some combination thereof? And five, what must be done from preventing it happening again?

My answers to your questions are informed by these two years of research. A significantly more detailed version of this testimony has been filed with the ONC.

ProgrammableWeb does not currently offer an API rather ProgrammableWeb maintains the largest independently run directory of over 14,500 APIs, but there are many more we don't know about. ProgrammableWeb also publishes articles for API practitioners, among them, various detailed accounts of API security exploits.

Many of the API providers we track offer publically viewable documentation. It is considered a best practice to offer such documentation as a part of developer and partner recruiting efforts. Even when an API provider doesn't offer official documentation for its APIs, a third-party might publish unofficial documentation. A recent example of this involved the APIs for remotely accessing a Tesla automobile.

When an API provider is looking to attract as many developers as possible, it usually does not concern itself with who can and who cannot access its APIs. In partner-oriented programs, the API provider usually knows exactly who has access to its APIs and for what reasons. Netflix is an example of such a program.

Developers are sometimes required to bear certain certifications to use an API. For example, PayPal's API terms of service say that API users must comply with the payment card industry data security standard, PCIDSS and payment application data security standards, PADSS and that that documentation evidence in its compliance must be provided upon request.

Twitter and other providers have similar terms about circumventing rate limits, a common defense against brute force attacks. In 2015 private photos belonging to several celebrities including Jennifer Lawrence were shared on the Internet after hackers allegedly penetrated a non-rate limited Apple API with a brute force attack. The hackers even publish the source code they used to perpetrate the attack.

Terms associated for PCI compliance or rate limiting are just two very small examples of such restricted terms. While thousands of organizations are racing to join the API gold rush, very few of them fully appreciate the difficulty in securing APIs. The belief or advice that if you rely on well-known Internet, web, and API security standards and best practices to provision your API, then your API will be secure has not borne out to be true.

Since 2014 many of the biggest Internet companies on the planet have either fallen prey to or discovered a major API vulnerability. This includes Google, Apple, Facebook, Pinterest and Snapchat. If the companies with the deepest pockets to employ the best experts are experiencing challenges in securing their APIs, how can lesser resource organizations be expected to successfully do the same?

When mobile applications are used, which involve a great many API cases, the majority of the API secrets that are shared between the mobile application and the APIs they call are easily discoverable, even when standard security technologies like HTTPS and TLS are thought to have secured their secrets. Certificate pinning, mentioned earlier by Google's Stephan Somogyi, secures this vulnerability, but very inelegantly so. Another major issue, the most advanced solutions for running APIs, homegrown or canned, are sometimes out of step with the most freshly baked API security standards. For example, those from the IETF.

Two key suggestions of mine are as follows: One, the maintenance of a centrally-distributed, constantly evolving checklist for not just securing APIs, but their adjacent...as well. This can inform key stakeholders on how to maintain the best possible API security, taking into account the very latest exploits. The same checklist could serve as the audit basis of some sort of Good Housekeeping Seal of Approval. In researching a majority of real-world API attacks that have taken place over the last two years, I have begun to formulate such a checklist.

Two, something must be done to ensure that white-hat activity does not end in criminal prosecution, but rather is encouraged through bug bounty programs. There are a great many ways and known best practices for securing APIs, far too many to enumerate in the allotted five minutes.

One important question, how do you instill confidence in consumers that their applications are safe to use? It is this very question that I ask myself and has provoked me to consider the idea of a Good Housekeeping Seal of Approval and all the elements that would make such a program successful. They are too long and detailed to cover as a part of this testimony.

Finally I don't think there are third-party certifying authorities that can be leveraged, but there are examples to learn from like the TRUSTe, NIST's Green Button Initiative and the PCI Security Standards Council. Thank you very much.

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

Thank you, David. Marc?

**Marc Chanliau – Director, Product Management – Oracle**

Hi, my name is Marc Chanliau and first of all, I would like to thank the task force for inviting my company, Oracle, to this hearing. I won't repeat all the good information provided by my colleagues on this panel and as a result I will try to keep this introduction very short. I am looking forward to participating in this discussion and answering any questions the committee may have.

Generally speaking we see two types of APIs; internal APIs, those are APIs exposed by product vendors like Oracle, to allow customers to customize or extend their vendor's product and integrate the product with third-party applications. This type of APIs is used by the vendor's customers and also by third-party vendors wanting to integrate their products with the API provider; in this case that would be Oracle.

And then there are external APIs and here we see two subcategories. The first one would be APIs exposed by companies to allow other parties to leverage their services. So examples of this would be FedEx or Walgreens. And then there are APIs exposed by companies to allow other companies to integrate functionality without having to develop that functionality themselves. So these companies make money out of providing APIs basically. So a good example is Twilio, as we heard from before on this panel and another example would be SendGrid.

Typically APIs are made public in open source or vendor documentation. By making APIs publically available, enterprises can improve partner connectivity, that so-called mash ups, and cloud integration.

Based on what I mentioned previously, Oracle only provides what is referred to as internal APIs. Oracle exposes APIs that allow our customers to integrate, customize and extend our product and Oracle's API documentation is publically accessible. For example, an internal API allows the developer to access session information that may be stored as part of the Oracle security products authentication process. The developers can then include that information in his own application, maybe an analytics application.

In addition to internal APIs, however; Oracle also offers products designed to manage and secure external APIs. These products are sold to customers seeking to ensure API security and management in their companies. These products provide services such as access control identity mediation between different identity schemes; for example, you can authenticate an API client using basic credentials and then transform this information into more detailed security tokens such as SAML assertions, to be processed downstream by backend applications.

One important part of API security includes audit, which enables service transactions to be archived in a tamper-proof store for subsequent inspection. API security facilitates privacy compliance specifically in healthcare, by allowing sensitive information to be encrypted or stripped out of message traffic.

API management, on the other hand, facilitates the creation of APIs that expose the functionality by backend systems and services. These APIs are published for use by application developers and are managed and monitored at run time. API management allows users to create APIs, it provides the ability to secure APIs, it enables easy API editing and publishing, it facilitates the discovery and use of APIs and it controls the access to APIs at run time.

This concludes my introduction. Now I am looking forward to answering any question or addressing any comment on the ONC com...that the ONC committee may have. Thank you.

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

Thank you, Marc. Shue-Jane?

**Shue-Jane Thompson, DPSM, ITIL Expert, PMP – Partner, Cyber and Biometrics Service Line – IBM Public Sector**

Thanks for the opportunity. My name is Shue-Jane Thompson, Partner for IBM Cyber and Biometrics Practice. We provided written answers; let me also summarize our key points.

Even though there is great fear about Internet accessible APIs, folks should not be afraid of APIs instead should leverage some API design to further enhance the privacy and security posture. Other than the regulatory issues, two main concerns are identity and trust. Of course today the breaches at large retailers and the cyberattack on OPM raised further concerns on API security. The reality is that if company failed to protect personal information, customer will quickly walk away.

IBM is the top leader providing security products and services. IBM partners with health industry across the public and private sectors and across all segments of market...all markets including healthcare providers, health trends set by science, health IT vendors, and federal health agencies such as HHS, the Department of Veteran Affairs and the Defense Health Agency. APIs are commonly used for internal application, also...business can be more challenging.

The need to secure the Apps and data flow is vital for healthcare clinical and consumer services. This is no longer just data at rest issue; I call that data in the air where data is exposed to the open. Yes, people are afraid of exposing their private data, yet when experiencing the technology advantages such as mobile Apps for making doctor's appointments, the ease-of-use is driving for more desire for additional features and requires for more data.

The balances of more data or more security when it is not APIs, considering want to...considering what to require, what data to pull, keep, share and dispose of are part of the API security equation. In addition, API opens up the boundaries between organization applications. The needs to...cyber threats, to spread across, there is a need to bring cyber CDC concept to the API level and better apply to the early detection of threats and ability to take preventative actions.

Well, how to better implement secure APIs? Let me share IBM, Alan Glinkenhouse has six common principles when he thinks about implementing APIs. One; should they be general APIs or customized APIs? Two, think about partners; who, what, and how? Three, leverage public APIs and available information. Four; leverage social data. Five, think about device level in the IoT environment. Lastly six, use the big data analytics.

Many of you may know that IBM has leading products that are designed to specifically tackle API requirements and challenges. In addition to the IBM infrastructure endpoint, data and application security practice, IBM had built an enterprise API management solution, EAPIM and allows for the creation of APIs by leveraging existing API building blocks.

In addition to our enterprise API system, IBM had created IBM Bluemix, which allows for individuals and companies to quickly create cloud-based applications. One of these features of Bluemix is the API marketplace. The marketplace is a tool that allows for developers to integrate premade APIs into their applications. Specifically for healthcare privacy, IBM also had Curam mobile Apps for healthcare case management.

There are ways to maintain doctor-patient confidentiality as personal information moves from APIs. Tools exist to anonymize the data as it moves from the patient or doctor's device through an API. This will be critical in order to maintain patient confidentiality. The use of session tokens and API keys can prevent unauthorized access to the information.

IBM is uniquely positioned from a software perspective as well as cloud capabilities such as SoftLayer when Bluemix technology and allows the users to implement single sign on capability, the identity source of the user can either be stored in IBM call directory through the SAML enterprise or social identity source.

The underlining cloud architecture is based on the SoftLayer call services. Softlayer allows for users to adjust the levels of security and IBM can help developers to ensure their applications are HIPAA compliant. Well, education customer is the best customer...I'm sorry, educated customer is the best customer.

APIs can be powerful and can be dangerous if necessary precautions are not applied. When I say precautions, it is not just about API development, but also the backend, called infrastructure and the governance. To address identity and trust, another consideration is to maximize machine learning, the machine-to-machine communications for advanced identity and trust evaluation. IBM Watson and BigML are by far the most recognized for machine learning and cognitive systems.

Finally, other than written answer we provided, a good book to read is from IBM and ...called "Digitalized Health Care." And there are several IBM webcasts available if you would like to do a deeper dive. Thank you for the opportunity to share.

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

Thank you, Shue-Jane. And finally, Gray Brooks?

**Gray Brooks – Senior API Strategist – General Services Administration**

Hello, can you hear me?

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

We can hear you.

**Gray Brooks – Senior API Strategist – General Services Administration**

Great, okay; so I will go through this fairly quickly and then I am happy to get into more detail in questions if it is helpful. So to the questions that you posed, first is does the organization which I represent, which I will talk about in a moment, use APIs for Apps which are available internally or to third-parties?

So, I work at the General Services Administration on a team known as 18F, one-eight-F. We are about two years old and are growing out the technical engagement within government for supporting other agencies. And so the answer to your question is absolutely yes. Basically every project that we do internally or externally that involves actual development begins with an API. It is a core premise of the team that you build the API first, make it available to all appropriate parties, and then build on top of that.

That...into the following question whether we publish our documentation online or make it available to third-party developers? Again, yes. It is our premise that undocumented API is of little use to anybody and that the documentation should exist as, you know, actual webpages on the Internet, public by default and available to as many people as can be.

So actually on the question of how we determine who gets access to our APIs? There are two layers to that. There is access to the documentation, and access to actually the material. Again, it is our belief that all APIs should be documented publicly by default; that there must be a compelling reason why documentation cannot be available publicly, in which case it should then still be available to the entire team internally.

As far as access goes the same exists with read access, the default is that anyone should be able to because of the opportunity that exists for innovation from places that we have not been. So even within the team of 18F, there are about 200 of us, if there is an internal API, it is documented in a way that anyone who is authenticated as a team member can access that documentation without having to request access.

Of course, it is different for write APIs; in those cases it is fairly straightforward that the people who have a need to write to the data source are the people who should be able to have access. We help run and then dog food our own service known as API.data.gov, which is an API analytics and key provider available to government agencies and we are...we use that for our own projects, internal and external.

To the question of whether there is a need for certification for privacy or security standards? Not distinct from the existing privacy and security standards that already guide our development. So the government and GSA have amply stringent requirement on that already and it is our view that APIs do not present a unique or different perspective from existing development, you know the API call is analogous to an HTML return when someone visits a page.

Similarly, where data is exposed, it is a question of are you making the proper decisions about what data should be visible publicly or to whom? And then, are you making the appropriate decisions about who should have access to edit that data? We find it more secure to actually not view. There is an unusual difference with APIs than just with every digital project on the Internet.

To the question of whether there are any specific language for privacy and security in our terms of use? It is our belief that by default terms of use are not necessary. Now if there is a compelling need that then is met by them, we have worked with our general counsel and with other experts in government to articulate what is a model terms of service for us; it is fairly light.

Our legal rights as the government are actually fairly strong already and there is actually a detriment to providing too much legalese to developers before they can access the web services we are providing. So, we instead try to use the terms of service that we have developed as a model as something that makes

more clear and explains the relationship to potential developers and it is fairly light and we have been reusing it.

As far as actual you know, privacy or security concerns or barriers to adoption of APIs? Again, in a sense it is not that there are any new ones that exist because of APIs; however, the same issues do exist of access and security and so some of the most important norms that we adopt across all of our projects, including our web services, everything that we build is HTTPS only; we force HTTPS, it is not an option. Then we provide API keys for our services, with a very low barrier of entry to get one, but we still do want that to happen.

API keys, you...it is important that they not actually be a barrier to adoption. If someone has to manually respond to a request for an API key that is going to be an encumbrance that interferes with organic use of your API. But it is very simple to have a form that requires e-mail and possibly if you to ask for a brief description of the goal of the project but, the person should then immediately have an API key and then we monitor how people use our APIs and can quickly respond if someone uses it inappropriately.

That gets more towards the question of risk mitigation. Again, monitoring all traffic, only allowing it through our API queue is a part of it. We have a default API rate limit that's in...I believe it is about 5000 hits a day; that is something that we adjust for projects where we are anticipating a need, and we really adjust on demand to anyone who requests it. It is not that our systems are actually fragile enough that that low limit is necessary, it just works for most people to get started and so we don't have a need to...we think that is a good baseline. Anybody could then request higher access and build off...

As far as the customer experience of third-party Apps go, using the API? Again I think we are focusing on the developer experience for our APIs and then trusting to them the customer experience they are making through their third-party Apps. By enhancing and maximizing the developer experience, we hope to drive as much reuse both internally to government and externally of our projects as possible.

But also, we think that is where we have the most role to play; we really do not get too terribly involved with the third-party development that is happening based on our APIs and instead trust that a multitude of mash-ups and reuse and third-party applications provide the best user experience by just being a multitude of different experiences people can use.

And then the last question, as far as third-party certifying authorities in the non-healthcare industry; unfortunately I am not in a position to speak to that. Again I think we have...we actually choose to have a pretty discrete line of kind of the way people validate themselves and that's just through the API key and then through human engagement with us, if we feel in the need.

We have not felt the need to have more certification for engaging with our APIs because we think that the best security model is one that focuses on the foundations, strong HTTPS, you know, a sensible and coherent model of access at every level and then, you know, good controls. The way we handle securities and our cloud management internally, etcetera.

So, that is a pretty fast overview of that material, but I am happy to get into more in the questions if helpful.

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

Thank you, Gray and thank you to all of our panelists on panel two. I will now turn it over to the task force to ask questions. Leslie Kelly Hall has a question.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Thank you very much, Michelle. So this group is very exciting to hear all of what you are doing and the cautionary note behind it. But I would wonder as your advice, we think about patients having access to the data, being able to transmit or share their data with others in care or their family members, or the people that they choose in any way that they desire, and the privacy that they choose. How could that be done without an API environment?

**Gray Brooks – Senior API Strategist – General Services Administration**

As far as how it could be done without an API environment, it would things that would have to go through static data, or, you know, really a non-machine-readable format. I mean, you could create a portal that allows people to browse and read and copy and paste. That, of course, is suboptimal. And there is something to be said for just bulk export not requiring an API that somebody is engaging with as well, but I think many of us on this panel would agree that the benefits of APIs is that you can actually track how people are using it and help them add a layer of authentication at different stages.

**David Berlind – Editor-in-Chief – ProgrammableWeb 21006**

This is David Berlind. I think that for those of us who have experienced this, you know, with our own healthcare providers, I visit...I have several doctors that I go to and it seems that each one of them has their own separate portal that is...where I can go back and maybe access information about my last visit or something like that; but that these portals are not interoperable. APIs fundamentally are what will help to kind of aggregate your medical graph, if you want to call it that, in a way that makes all the information from all of your healthcare providers available sort of in one query.

So, I think that when I look at my primary care physician and their portal, it would be relatively easy for my family member or anybody I want to share the information with, I could give them access to that portal and no APIs would be required in the instance. However, to really get the benefit of seeing the big picture of my health and being able to share that with whomever I want to share, that itself would require APIs so that the data could be drawn from multiple repositories where that information is being stored. Proprietary interfaces, which are the other way of sharing information, would essentially present a degree of friction that would make that sort of interoperability on a grand scale across all patients and all citizens of the United States virtually impossible.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

So really what you are saying is we can continue to do the wrong thing well or we can figure out how to do something new better.

**Gray Brooks – Senior API Strategist – General Services Administration**

Yeah, I want to be clear that, I know that I issued some cautionary notes about the state of the state of API security, however, I think I heard it in the earlier panel, you know, just about every technology is presented with sort of a trade-off of...no technology is intolerable and so at some point we come to a decision as to whether or not the efficacy of the technology outweighs the risks associated with using that and I believe that to be true of APIs.

**Marc Chanliou – Director, Product Management – Oracle**

I just want to make a...this is Marc Chanliou here. I just want to make a quick comment; the API gives you an entry point into an application reading, so to answer or to address your confidentiality issues and all the concerns you may have about privacy and so on and so forth, this is already handled by the backend application that is going to process your request. The API is here to allow you to make that request through that API or the application that is going to process that request.

So there are two levels of confidentiality here; there is the confidentiality about the API itself, and that needs to be protected through authentication, authorization and all that good stuff that my colleagues have talked about. And then there is the application at the backend that is going to process the request itself and that application also needs to be secured accordingly, to preserve confidentiality and so on and so forth. So you have got two stages there, the API stage and the backend application that deals with the request itself.

**Shue-Jane Thompson, DPSM, ITIL Expert, PMP – Partner, Cyber and Biometrics Service Line – IBM Public Sector**

This is Shue-Jane; I would like to add another comment to this...that I think this as an API ecosystem and internal APIs, public APIs and then even within one organization there are multiple APIs have that intricate relationship. We have seen, the industry practice here is, in order to look into the interoperability access, some of the private sector have established something called Care Everywhere, which is, you know it is not necessarily based on the API but in the general consensus outside of EPIC was that it was a closed network.

And, you know folks can work together in terms of establish that ecosystem and establish agreed upon rule sets. Kind of goes back to what I said, this is almost is a cyber CDC has been extended to, you know the API level. So this ecosystem will require additional attention in order to add this necessary data protection.

**M**

Hi...

**David Berlind – Editor-in-Chief – ProgrammableWeb**

Yeah also, again this is David Berlind. I just want to point out that there are so many different security frameworks at multiple level depths if you want to call it that, because I heard that word used earlier, that apply here. In most of the research I have done over the last two years, the majority of the exploits of the vulnerabilities came as a result of some human error, right? And that was the point of what I said in my testimony was, which is that it's in the largest companies have had either a vulnerability or even worse, an exploit and in most of these cases like for example, where rate limiting was not applied to an API which allowed for a brute force attack, we are talking about human oversight.

So, we can have a lot of these great security technologies and frameworks in place however, they have to be accompanied by a set of best practices to ensure that the security and the privacy of the data involved is maintained. An example would be, you know when you take into account the way PCI DSS works, you know, if you are keeping credit card data, then you have to comply with a certain security checklist.

If you're not keeping that data, then no big deal, I mean, you can imagine that the same thing would be true of, in a healthcare context, an EHR context where by the...if you are using APIs to get at some data

and that data flows...you get to the patient or the patient's data or the patient's doctor, but you don't store that data, that is a very different process requiring different degree of security . to your And EH our context whereby, if you're using the API and you get to the patient or the patient's doctor but you don't store the data that's a very different process requiring a different degree of security than if you take that data and you hold that data in your system somehow. So, I just want to impress upon everybody that there's...there's really the problem at hand or the challenges that...here are very much twofold, it is about the technology and the degree to which the technologies are prepared to secure APIs and then the best practices and the extent to which they are widely shared and complied with in sort of a standard way.

**Aaron Miri, MBA, PMP, CHCIO – Chief Information Officer – Walnut Hill Medical Center**

This is Aaron Miri; I am one of the members here of the committee and I just want to also add on to what you just said there. And I think another point that I believe we have all sort of talked around, but we are making the assumption of, is that the data is readily available to be accessed by the API and thus shared by the API. I just want to be...I think it is good for the record to state that, again I said kind of earlier that a number of data sources within healthcare are very much closed-loop systems.

So we are assuming that an API can exist that will be able to access the data and best transmit it to whatever other system, as appropriate, at the whim of the application or the user using the API. So given that, all of this must, you know, we are taking with a mindset of, the data is available, but I believe that is also a fundamental challenge we are going to need to attack at some point is making sure that that data can be transmitted, given how much of a closed-loop system healthcare systems can be.

**Alisoun Moore, MPA, MBA – Senior Director of Corporate Development for the Federal Sector – LexisNexis, Inc.**

This is Alisoun Moore fro, LexisNexis. I agree with the comments that the API is sort of your entry point. And I also agree with the comments that many healthcare systems are closed-loop systems. If you want to be able to share data healthcare provider to healthcare provider, even at the behest of the patient, you have to be able to not just technologically be able to access the data sets that each healthcare provider owns, but then you must be able to authenticate that the patient record that you are trying to access across many providers is the patient that you are trying to access.

And, I think that that could be accomplished on the backend with the ecosystem that I think another panelist had defined. But you have to be able to authenticate that John Doe is in fact the John Doe you are talking about, so that you don't inadvertently access the wrong patient records and transmit that to whomever, which may be an issue at that point for that particular provider.

**David Berlind – Editor-in-Chief – ProgrammableWeb**

That particular use case is the sort of use case that would be, in many cases, governed by the issuance of an OAuth token whereby the OAuth token represents the intersection of a user, let's say a patient, and a particular system that has data belonging to that patient and then that system would issue a OAuth token to a third system or application needing access to that data.

And, you know, the thing that got me started on the API research that I was doing was a very large scale attack that was very highly publicized and showed up on Twitter and Facebook whereby the hackers gained access to the OAuth tokens, the Twitter and OAuth tokens belonging to tens of thousands of Twitter and Facebook users because the application to which they had been issued, the service to which they had been issued, was storing them in an unencrypted format in their database and that database

had been broken into. And that allowed the hackers to impersonate the users of Twitter and Facebook in a way that the hackers were allowed to make unauthorized posts on their behalf. So this again is a best practice, right? It is, I think I heard earlier that...

### **Multiple speakers**

(Indiscernible)

### **Alisoun Moore, MPA, MBA – Senior Director of Corporate Development for the Federal Sector – LexisNexis, Inc.**

Yeah, there are multiple ways to be able to authenticate identities, right, on the backend systems and many of those ways do not involve a token. But I agree, the...out there, and we deal with them every day, they are really sharp and you have to stay ahead of them, I think as the, I think it was the Google panelist earlier, you have to be forward-looking at what they are going to try.

But there are many mechanisms by which you can accurately identify and resolve, you know, patient identities across many systems. So I think what we are saying collectively is, your API is your point of entry, but behind that we should have a shared ecosystem that the various organizations buy into with the appropriate authentication that need to occur patient to patient and in other cases, provider to provider and then patient to patient, almost a two-tiered structure.

### **Shue-Jane Thompson, DPSM, ITIL Expert PMP – Partner, Cyber and Biometrics Service Line – IBM Public Sector**

I totally agree with that assessment. In addition to that here, this is what I was talking about, the machine learning and cognitive technology, because our environment is very dynamic, right, in nature. And so this authentication trust establishment really requires that continual learning, continual assessment and evaluation of the...so this is not just an ecosystem, this is really multiple ecosystems, the ecosystems really don't stay static.

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

Josh Mandel has a question.

### **Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

Yeah, so first off just thank you to the panelists; I really enjoyed the presentations and the discussion so far. I wanted to react to what I thought was some very deep and clear thinking on Evan's part about what it takes to standardize the API.

And just for folks in the panel who may not be following the regulatory environment for healthcare data access as closely as we are supporting ONC here, as part of the next stage of the Meaningful Use process called Meaningful Use Stage 3, there is a certification program that will require EHRs and clinical provider organizations to expose data to patients using some API, but there is no attempt to standardize what that API will be. It is described as sort of a functional requirement; so everybody has to offer an API, it has to be documented and it has to have certain basic features like letting a patient search for their medication or search for immunizations that they have had. But they don't have to do it in a standardized way.

So that's where we are today and there's pretty broad ambitions about how we would like to get to a future where there is more standardization. But as I have described sort of an interesting distinction

where different parts of an API specification might evolve at different speeds. For example, the serialization formats could be crystallized quite early, but the request and response sort of payload mechanisms might be something that is left in flux or that is tied down later in time; that kind of thing.

I am curious whether any of the panelists have experience with these kinds of attempts to standardize APIs. Most of the consumer Apps that I have seen, you know, there is only one Facebook and so if you are writing a Facebook App that connects to Facebook and ditto for Twitter and Google Docs and many of the APIs we work with, as consumers, on a daily basis. I am wondering if anyone has experience in building standardized APIs, and whether there are special considerations in that domain.

**Marc Chanliou – Director, Product Management – Oracle**

Well, I think what we standardize today is API security, you know, using various standards, Open ID Connect, OAuth, SAML and, you know a...to access user information and so on and so forth. In terms of designing the API itself, I am not aware of any standardization on that front, but as far as security is concerned, of course yes, there is standardization through, you know, the number of standards are enumerated before and I think every person on this panel will concur to that; we all use the standards in some form to protect access to the API. So that's where the standardization in my view is taking place, in the security around more than the design of the API itself.

**David Berlind – Editor-in-Chief – ProgrammableWeb**

In the UK there, as mentioned earlier today I think in the Q&A session after the first panel, there is sort of one of a kind project in...whereby the UK government has...is enforcing the creation and then compliance with a standard API that all the banks in the UK have to comply with. It is primarily a data portability and the consumer protection issue; so, if all of your data is...if you are keeping all of your financial data with one bank and you decide you want to move to another bank you shouldn't have to you know, unload your applications and all of that, you should be able to access that data relatively easily without having to make a lot of changes. So and there is a project that is sort of, in the UK, that inspired that called the Open Bank Project.

So, I don't know of any other similar standard APIs have appeared in the US; however, I would say that one thing that we do at ProgrammableWeb where we are changing our data model actually to address this trend, we see these APIs that we call meta-APIs. And so if you think about that single-purpose API like let's say something from a storage service like Box or Dropbox as being kind of a model API, a single-purpose API. But then we could use meta-APIs which attempt to give developers a single API for accessing multiple dissimilar APIs that are roughly the same thing.

So a meta-API in a storage market might support Google Drive, Dropbox, Box, all of these storage services that in and of themselves have very different APIs but, if you are working with a meta-API, there is one API that kind of multiplexes all of those. So, it deals with the dissimilarities between the various services in a way that eases the burden on the developer to kind of do things like...when one service is down to kind of pick up your data from another server, that sort of thing.

So, while I haven't observed any of these standard APIs, if you want to call them that, in the US, other than certain ecosystems like OpenStack, I think what you see is the API ecosystem evolving to create standard APIs to resolve such differences.

**Evan Cooke, MS, PhD – US Digital Service at the White House**

This is Evan Cooke and I want to thank Josh for his question and potentially present a way or a framework that may be helpful in thinking about this question. And that is to go back to an analogy that was raised in the panels earlier today about thinking about APIs as software contracts. So, if we are considering an API or a standardization or certification or API for a certain scenario, what if we perform a thought exercise where we place the technical API with a contract between the parties that are participating in that API.

What parts of that contract do you want to be static over the next time period, say it is six months, say it is a year, say it is multiple years; what parts do we want to change? And if we have a standardization process and we have a process whereby changes will be accepted, integrated and then deployed into revisions of the protocol, are those timelines consistent with what we expect portions of that contract to evolve?

And so that is a helpful way to potentially analyze a scenario and say yeah, a codified, standard contract that we believe will only change every year, is actually what we would want in this scenario, therefore, we could propose a technical API specification that is relatively detailed to implement that contracted software. Thank you.

**Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

Thanks.

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

Aaron Seib?

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

You know, Josh's question actually echoed a lot of mine so I will pass.

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

Okay, thank you. Meg Marshall ?

**Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation**

Hi. Yes, thank you. And I would like to echo all of the gratitude toward this panel as well, this is a great conversation. So my question is kind of circled around this a little bit maybe in a prior panel as well just around this whole consumer protection thought. And, you know, the idea that the patients in particular who may be accessing, but it could be providers as well, perhaps have limited resources, potentially limited technical savvy and I would like to maybe point toward a comment that you made, David Berlind, around a Good Housekeeping Seal of Approval.

You had mentioned that you put some thought into this and that you thought about some of the elements that would make a program successful, but they were too long and detailed to enumerate today. I am curious if you could give us a high-level overview and then maybe share with us how you could potentially provide us that more detailed response.

### **David Berlind – Editor-in-Chief – ProgrammableWeb**

Yes, sure. So again, as I think I mentioned earlier, most of this thinking is driven by just watching what's going on in the real world and saying, okay, well there's another thing that, you know, nobody thought of or nobody is paying attention to. So with every exploit you sort of reverse engineer the exploit and then once you are done, you have got a list of things that you need to look for. For example, rate limiting or encryption of token, you know OAuth tokens at rest or use of hardware security modules to secure certain secrets.

Just this month, we have had two pretty major API vulnerabilities revealed. One of them was with Verizon's Hum service where the credentials to access the APIs were plainly visible in the source code of the website. So you could have...that is a checklist item, have you reviewed the source code or has a machine reviewed the source code and you look for user ids and passwords?

There's...some of these exploits involve compromise of source code repositories that were deemed private and kept on GitHub, so, are your credentials for the APIs or anything secret, being stored in plain text in those...source code repositories? Are the source code repositories protected with two factor authentication so that the only people can access them are the developers that are authorized to access them?

These by the way are not things I am making up; these are all surface...parts of the surface area that were penetrated by hackers in real-world exploits. So, and part of the real key important thing there is, it is not just the API itself that in some cases might be vulnerable, it is the adjacent things around it. The hackers, you should realize, will stop at nothing if it is deemed the data that they are going after or whatever it is the objective is to be very valuable.

And so to the extent that this data we are talking about here would be valuable to some hackers, they will orchestrate a very sophisticated attack that involves multiple barriers that have to be breached in order to get to the final objective. And, some of those barriers may be directly...may directly have to do with the security of the API itself and some of them will have to do with the adjacencies.

So this checklist that I am envisioning covers not only all of the things that we know about, but all of the things that we do not know about. So for example, tomorrow we wake up and we discover another API attack or some sort has taken place and we reverse engineer it and we find two things that are not on the checklist. And so, in my mind there must be...it could be a program, essential clearinghouse of some sort, a nerve center whereby you are constantly evolving a set of best practices that are designed to inform all stakeholders about not only what they should be looking for in their existing systems, but as things happen, what the new things to be looking for are.

This program would include a clearinghouse of all the exploits, detailed information about what was...how they were perpetrated, education, you know, how do you do this? Setting standards, standard participation for example, at the IETF, so that you are letting the stakeholders know, hey, this stuff is happening in the IETF, here is what you need to know about that and how you should be thinking about your existing systems that we will need to adjust once these standards are ratified.

Email services to the community, you know you establish a community that you, as a nerve center, you are pushing information out to your community as opposed to waiting for them to come to you. This checklist could offer service sort of like almost like a prescription for companies that either build API management solutions that have security functionality baked in to them or for those companies who

choose not to use the canned solutions and choose to home grow their own API solutions and there are many of those.

**Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation**

Thank you, that's very helpful. And if I may follow-up with that maybe for a little more clarification and certainly open it up to any of the other panelists as well. So one of the things we are looking at, the use cases and we've explained a little bit the Meaningful Use Stage 3 requirements as EHR developers will be allowing consumers to access their own clinical data on an App of their own choice that meets the EHRs technical specifications.

So I suppose I am trying to bridge these two concepts you know, in your testimony David you mentioned the large sets of unknown developers and it sounds as are hearing...as we are learning throughout the day, it sounds like a fairly tight connection is going to be needed between the API developers, and the clients, and then certainly the patients to describe what these terms of use are and what these expectations are, whose responsibilities lie are where and then certainly an education component with the patient himself.

So I am just curious, do you see a path moving forward that does not leverage a quote unquote "Seal of Approval" or something that, you know what is it the easy stamp or the easy button; something that is very quick, very visual, very easily understood mechanism, especially from the consumer's perspective. But from the providers as well that says, this is safe, this is easy, you can trust it, let's go ahead and use it. Do you see a path forward without something like that?

**David Berlind – Editor-in-Chief – ProgrammableWeb**

Okay. I am not sure I would be confident moving forward as a consumer. I want to be clear that a Good Housekeeping Seal of Approval, which I didn't address in my prior answer, sort of cuts both ways. What I mean by that is, if I am a user, an end user of an application and I would like to know that that application has been certified by some third-party to protect my privacy before I use it; something along the lines of what TRUSTe does for e-Commerce web sites.

I think that it also cuts the other direction, not only is the Good Housekeeping Seal of Approval good for consumers to know which applications they can trust but there also should be Good Housekeeping Seal of Approval on the APIs themselves so that developers know that they are working with an API and an API provider who has taken all the necessary measures to protect the data that is deserving of protection.

Now, can you move forward without a Good Housekeeping Seal of Approval? Sure, I mean, we see that all the time, plenty of ecosystems move forward without something like that. But as somebody who is deeply familiar with the risk of APIs and the risks of data going public that sort of thing, and seeing it happen on almost a weekly basis, my confidence is already rattled and I would be very, very hesitant to do business in a way that would reveal my personal health data, that might reveal my personal health in a way that I did not intend so I would like to see something of that nature, like Good Housekeeping Seal of Approval.

**Drew Schiller – Chief Technology Officer &Co-Founder – Validic**

Hey guys, this is Drew Shiller. I just want to say, I completely sympathize with the sentiment and agree, by and large. I do just want to caution us from going down a path where we are creating a new regulatory body that is reviewing the thousands upon thousands of potential applications that we could

be getting for new use cases of this. I just think, that I agree that there is a seal of approval potentially there but you know, TRUSTe is an example of a commercial entity that stepped up to fill a void that was there. And so I think maybe we could think about how to structure some guidelines and then maybe some independent third-party services would crop up to actually provide some of the certifications.

**Alisoun Moore, MPA, MBA – Senior Director of Corporate Development for the Federal Sector – LexisNexis, Inc.**

And I...this is...

**David Berlind – Editor-in-Chief – ProgrammableWeb**

Yeah, I agree; there are challenges of scalability here. I think it's more...yeah, go ahead.

**Alisoun Moore, MPA, MBA – Senior Director of Corporate Development for the Federal Sector – LexisNexis, Inc.**

I want to commend David, you have excellent comments regarding what...go after and I understand the task forces, what appears to be your desire to have a standardized interface for consumers, sort of that Green Button, so to speak.

The question I have is, you would...to get that seal of approval, you would have to have certainly safeguards or standardization on the API. So the question for the people who actually own the data, the providers on the backend, their systems as well would have to be very secure for patients entering through that type of API. So, would it...isn't it a two-tiered structure that you would have to ensure with the security of the data and privacy of the data is protected?

**David Berlind – Editor-in-Chief – ProgrammableWeb**

Is there a question there?

**Alisoun Moore, MPA, MBA – Senior Director of Corporate Development for the Federal Sector – LexisNexis, Inc.**

Yeah, it's, you know, if you think about the...what we think about is yes, we would like to provide our clients with a standardized API, right, so anybody that signs up who wants to access LexisNexis data, who wants to share with us their data and so that we can run analytics against it so to speak, and we have a standard API.

But behind that API, we have a standard interface that is secure, but behind that we also have a massive amount of infrastructure security, application security, that for somebody who hosts the data, you know, is responsible for any breaches of that data pass the hat. So, API we are allowing standardized access to patients as one mechanism of an entire sort of security, secure infrastructure so the clients will be happy but, the entity that is liable or on the hook for a risk of breach is actually the provider who is allowing that access.

**David Berlind – Editor-in-Chief – ProgrammableWeb**

That's right; I agree with that. And I think that, you know, the point I was making earlier there was just that, you know LexisNexis is, you know, you started talking about the layers where various securities apply at the infrastructure level, etcetera. And some of these things all contribute to the various layers that end up being API security. We heard, you know, access control for example might actually be subjugated to something like SAML or active directories. Ultimately, that plays a role...that could play a

role in what the API has, you know, which people are coming through the API and what they have access to, right?

**Alisoun Moore, MPA, MBA – Senior Director of Corporate Development for the Federal Sector – LexisNexis, Inc.**

Right.

**David Berlind – Editor-in-Chief – ProgrammableWeb**

And so that is a layer in that. However, you know, I just want to point out is maybe if we created a checklist and presented it to you, you would score, LexisNexis would score 100 and that would be great. The question is, how do we know that everybody who is a part of this ecosystem, who is...every provider for example who is potentially in a position to reveal data also gets a score of 100 on that checklist.

And as I pointed out earlier, in most of the vulnerabilities that involves from the very biggest API, very biggest Internet companies that have the most money to spend on security resources, is all human oversight. It was an oversight in the development of the API, it was an oversight in, you know, one security setting, it was an oversight and so, that is why these checklists are so important.

And that is why I think having...such a checklist doesn't exist; if it does, we would have reported on it already at ProgrammableWeb, it is why, you know, we started thinking about this idea because boy, if the biggest companies out there are having difficulty securing their APIs, then what does that mean for the rest of us? And as you know, the EHR ecosystem is huge in terms of the number of vendors that are participating...

**Alisoun Moore, MPA, MBA – Senior Director of Corporate Development for the Federal Sector – LexisNexis, Inc.**

Yes.

**David Berlind – Editor-in-Chief – ProgrammableWeb**

And so some of those companies are startups and may not have the resources that the bigger companies have. You know, that element of you know just leaving those companies to their own devices to get it figured out introduces a fair amount of risk for the entire ecosystem, if you ask me.

**Alisoun Moore, MPA, MBA – Senior Director of Corporate Development for the Federal Sector – LexisNexis, Inc.**

Well there is a, you know, if you are a covered entity, right, under HIPAA, there is sort of a regulation that has security provisions associated with it that covered entities must abide by. So I think you are talking about a more significant checklist and more of an assurance, if I am not mistaken.

**Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation**

Yeah, I don't think...be able to make the assumption that...

**David Berlind – Editor-in-Chief – ProgrammableWeb**

Maybe...the checklist that people just use it themselves and it is not necessarily an enforcement or Good Housekeeping Seal of Approval but it's just like out as education, hey guys, we are all in this together, which by the way there is an issue, an industry-wide develop an issue with disclosure. When something happens, there are various degrees of disclosure.

I think disclosure is very important in order so that everybody so can learn. But in our research, you know, we have had some vendors come forward and say, here is exactly what happened to us. And then we have had other vendors that come forward and sa...and look us, just literally say, nothing happened; meanwhile, evidence of a breach is in full public display. They will say, sorry, we don't...there is nothing to talk about. So...crap.

I would also like to point out that in the media business, which I am a participant in and I am sure all of you are familiar with this. You know, people have various what the call graphs, right? You have your social graph, you have your commerce graph, you have your business graph, and these are the...this is all the connective tissues that kind of your personal graph on Facebook, you know all of friends that are connected to you and who they are connected to, that is all part of your Facebook or your social graph. We all have an American graph and, we have a variety of these graphs.

Now in the media business, there are companies, sort of sneaky companies that you will be like, wow, they are doing that? Where, even though certain informa...certain graphs of you will have been anonymized in a way that if you look at that one graph, you would not be able to tell who it belonged to, they are able to join it with another graph and suddenly identify who it belongs to, who that data belongs to.

**W**

Yup, that is true.

**David Berlind – Editor-in-Chief- ProgrammableWeb**

I know, and you know in leading up to this hearing, I was reading about how, for example, the Obama Administration is pushing hard on the cure for cancer and part of the imperative is to open up a ton of this data that is hiding in the systems, anonymizing it of course, but opening it up in a way that the data can be looked at from a big data perspective to mine out some things that are not necessarily mi...you know, that doesn't necessarily come to the surface when you are trying to cure cancer.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

It's also, I just might want to add some clarification; this is Leslie, that includes a patient consent in that participation, just so that the others do know.

**David Berlind – Editor-in-Chief – ProgrammableWeb**

The question that comes to my mind is, if you, you know, can various medical graphs or other graphs be connected in the same way that the media industry does, to suddenly identify somebody that you didn't think was previously identifiable, because of the way the graphs have been anonymized. I don't know the answer to that question that are connected the only way that the media industry does to say that question, I am just saying, people...there are sneaky people who work very hard at solving that problem.

**Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation**

Yeah, this is Meg...

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

Josh Mandel...one more question? Sorry Meg.

**Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation**

I think that is very interesting and maybe one of the things that we could do as a task force is we could work with OCR and our wonderful subject matter experts with ONC and others at HHS to provide some clarification around some of those things. When we looked at developing the questions, we had originally included one around, you know, legal barriers or obstacles or concerns and then we decided to take that out.

So maybe one of the things I think would be helpful and for any of the panelists who want to continue to listen in to the task force meetings as we follow-up and aggregate the recomm...and create our final recommendations, it would be helpful to kind of close that loop and have some of that expert guidance on a few of these topics that I think are being raises that maybe have answers out that we do not have the ability to draw on them right now. So Michelle and Rose-Marie, if we could just kind of put pins in those in particular, we could probably get that sorted out fairly quickly.

**Shue-Jane Thompson, DPSM, ITIL Expert, PMP – Partner, Cyber and Biometrics Service Line – IBM Public Sector**

Well if I may add to that, I think the reality here is that we understand that hackers and actors will continue to evolve, right? Other than we going back to the basics and not displaying our credential data in the clear or ensuring the access control, I think there is a very complexity that we, you know, as part of this so-called ecosystem if you would is that continue evolving the different vectors of threats, you know, for us to be able to provide that data.

I love the fact that we talk about nerve center, right, this is nerve center had gaps and complexity that even discussed, you know, in a different so called sphere of organization, cannot solve along. And so, this is where I talk about this so-called, you know, machine learning, machine-to-machine communication, creating that so-called almost social network base, you know, probably recognizable credential system so we can verify and evaluate the trust and the credentials for each of the entities in the different levels.

I think this is where cognitive technology comes into play. This is where machine learning comes into play. I think in our...panels, you know, subject area can really further look into that the area of technology. It is greatly needed.

**Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation**

Yes, that is very helpful. Michelle, do we have other questions in the queue?

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

Yes, we do have a few questions in the queue.

**Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation**

Okay.

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

Thanks, Meg. Josh Mandel?

**Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

Thanks. I had a question to follow-up on the discussion about white hat hackers and how do we promote exploration without punishing people who are trying to do the right thing. You know, back in 2014, I found a vulnerability that seems to affect a great number of EHRs out there and when I tried to contact the security teams at upwards of 80 vendors, I had a very hard time even figuring out how to get in touch with them; lots of bounce backs from security, mailing addresses, and no clear procedure.

I am wondering if the panelists have concrete ideas about what we could do to improve this, whether it is through a list of best practices and sort of checklist items or whether it is through a regulatory process. But what are some concrete things that we can do to make it clear to vendors; number one, that they need a way to take in these kinds of security reports but also then to share what they have learned so that we do not see the same implementation mistakes over and over again?

**Alisoun Moore, MPA, MBA – Senior Director of Corporate Development for the Federal Sector – LexisNexis, Inc.**

Hi, this is Alisoun, I will take a first stab at that. We know in some of the other industries, like healthcare payers which are vulnerable to quite a lot of fraud because they are the ones that actually distribute checks, right? They have created, actually with...along with CMS, the Healthcare Fraud Prevention Partnership, which is a combination of both private and public payers. And that was created to specifically do what you just said, was to share vulnerabilities that have been uncovered by a member with other members. Okay? So that's one example.

Another example is in the, again where you have industries that are paying out money, which is what...like to focus on; in the property and casualty markets, again, they did the same thing. They sort of treated the contributory...voluntary contributory sharing of data where they share with each other those types of attacks and that their, what we call special investigative units, CSIUs within those companies share that information with each other, they know pretty much who to go to and where to go to and where that information is stored.

It is just a suggestion to perhaps borrow from some of the other industries that have run into the exact same issue you are talking about. And we do assist those, as do many of the other panelists that you have heard today, in some of those efforts.

**David Berlind – Editor-in-Chief – ProgrammableWeb**

Yeah, I think one, this is another example of where a nerve center of some sort could come in really handy, somebody who knows the entire community, you know, and can get the information to the right person as quickly as possible. But on the other hand, I think that companies like Google and I know Stephan Somogyi's kind of maybe still on the line or not, could address this. They are probably the most advanced of the companies in terms of promoting white hat activity research and they offer a bounty, depending on the degree of the severity of the find, an example being in April 2015, a developer discovered a way...

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

I am not sure what happened, I think we lost him.

**Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

Yeah, I think so.

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

Okay, well, we do have other questions in the queue, if there are not any others that want to respond.

**Evan Cooke, MS, PhD – US Digital Service at the White House**

This is Evan, I will add a quick note here. I would also urge the panelists, to the extent that they haven't already, to take a look at some of the great work going on under the Precision Medicine Initiative happening inside of HHS as well as across the federal government. And specifically some of the privacy policies as well as other work under way, thinking specifically about some of these issues about reporting as well as vulnerability disclosure.

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

Thank you. Leslie Kelly Hall has a question.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Thanks, Michelle. I really appreciate the comments about the ideas for checklists and the ideas for somehow giving people the ability to be more competent. It seems as if many of the breaches noted were oversight or human oversight or not using best practices. We had heard about E Trust and HITRUST and I think the content area, URAC is one area that they do some sort of Good Housekeeping Seal. And I think that all of these things are still based on some foundation of regulatory framework or minimum standards there. Can you guys speak to what you believe where that line of government starts and stops?

**David Berlind – Editor-in-Chief – ProgrammableWeb**

This is David, by the way, I am back.

**Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

...would you begin to resummairize that question?

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Sure, I am just really wondering, all the examples given, E Trust, HITRUST and others, there is still some underlying regulatory minimum that they are building upon. It is not just solely an industry response; banking has banking regulation, FTC has regulation and I am asking the group where they see that line is? Where do they see is appropriate as we enter into this new ecosystem that includes patients?

**David Berlind – Editor-in-Chief – ProgrammableWeb**

Well, this is David again. I think some of those organizations like TRUSTe are commercial organizations...

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Yes, but they are still responding to governmental...there are still some minimum data sets through minimum standards in banking. There are still minimum things that have to be done.

**M**

Right.

**Alisoun Moore, MPA, MBA – Senior Director of Corporate Development for the Federal Sector – LexisNexis, Inc.**

This is Alisoun. I would agree that there is a role for a regulatory framework, I believe it does exist with the passage of the HITECH legislation and the ACA regulation, along with many other regulations addressing privacy and security. I think with the HITECH, NIST has a very clear role in certification of EHR systems. I think with the HIPAA law there is definitely a very clear role of what is required by anybody who transmits health information electronically that is required of them. I think that you are correct, there is a regulatory framework. The question is, does it need to be strengthened or does it need to be deregulated?

I certainly would not put myself in a position of being able to answer that. I think we will have some lessons learned by all of the patients who, including myself I might happily add, who now have access to our historical records from my provider and I am ecstatic about it because I can now see the entire thing for over 10 years, which didn't exist before HITECH was passed. So I think as this evolves, there will be further adjustments to that regulatory framework that is already in existence and perhaps even some new regulation, if there are some egregious issues that arise from usage and access from patients to these systems.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

This is Leslie again, I just think the flipside of that also has to be considered; the fact that people are now in the dark, patients in the dark, providers don't have all the information. It seems the risk of lack of information is greater than the risk of having information and presenting it in a responsible and secure way.

**Alisoun Moore, MPA, MBA – Senior Director of Corporate Development for the Federal Sector – LexisNexis, Inc.**

Well I would say that the lack of information, and I will speak anecdotally from my own experience, usually comes because my particular provider, unless there is an affiliated provider with that provider, the information if I go see a specialist outside of that network, they will not be able...I cannot see that information unless I access the system. So if you are depending upon proper care access to your full medical record, I think it is critical and I think one of the challenges we have before us is being able to share that information across many providers.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

Thank you.

**Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

So this is Josh. I was wondering now that David has reconnected, if we could come back to my earlier question, because I know that he was just beginning to share some thoughts about what would be concrete steps we could take towards making security vulnerability...

**David Berlind – Editor-in-Chief – ProgrammableWeb**

Right; I apologize, Verizon must have heard me make that comment earlier and disconnected me. So I think what I said was one, this a world that a nerve center could play a big role in in terms of sort of being a clearinghou...not only promoting bounty programs on behalf of the community, but then as essential place that you could receive information from researchers and white hat hackers, if you will.

I want to point out, the reason that I made that comment in my testimony is because developers that I had talked to in preparing for today mentioned that they will never research...they will never conduct anonymous or unprovoked research if you will, against health system APIs for fear of criminal prosecution. I don't know if there is a reality there or not, but my understanding is that if you attempt to penetrate, do a pen test if you will on a healthcare system that that activity is then has been somehow criminalized. That could be reality or it could be a perception; either way, it has to be changed because this white hat activity is a very much the activity that protects the Internet infrastructure and many organizations and needs to be encouraged, not...and incentivized as opposed to discouraged, whether legally or not.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

This is Leslie, I would like to follow up in that the new OCR guidance is something worthwhile to read. There is a lot of information that this group has touched on that I think has been clarified quite well and really promotes the idea of this open ecosystem.

**David Berlind – Editor-in-Chief – ProgrammableWeb**

That's good to hear. Like I said, I don't know about that, all I know is what some developers that I interviewed told me and they were like yeah, we will hack away at Google and Yahoo and Apple and Microsoft, but we won't touch the healthcare stuff, right? So, and that is not a very good perception. And then of course, like I said, you know, you probably to kind of go from zero to 60, you would want to talk to the companies that run very good bounty programs, like Google.

And I think as I was saying when I was cut off is that in April 2015, a hacker, white hack hacker discovered a way to wipe out all the videos on YouTube through the YouTube API. And fortunately, he discovered it before anybody else and reported it to Google, which has a very official process for doing that, and depending on the severity of your find, you get paid a certain amount of money. And he said in the reports about what happened in a blog about this, Google got back to him within like minutes; like it was a very fast response and they shut down the vulnerability very quickly. And that of course is the sort of process that you would want to aspire to in the healthcare industry. I don't know if that answers the question.

**Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

Yeah, I think it was quite helpful; thank you.

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

Aaron Seib has a question.

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

Yeah, I just wanted to, you know we talked a little bit about the Good Housekeeping Seal of Approval and a checklist and I just, you know, we also talked earlier with the panel about when you are sharing data, there is always a risk. I think an important part of that checklist would involve consumer education, right, about the risks that they are taking when they adopt technologies, which we of course want to encourage them.

Question to the panel is, are they familiar with any consumer-facing educational materials that might help us advance that and make sure consumers understand and have a knowledge base of the risks that

we are reducing and the risks that will persist and the unknowns? Are there any decent consumer-facing educational materials about sharing sensitive data?

**David Berlind – Editor-in-Chief- ProgrammableWeb**

I think that is a great question because despite everybody's attempts, the entire security community's attempt to educate the world on how to not fall prey to phishing, e-mail phishing...

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

Yeah.

**David Berlind – Editor-in-Chief – ProgrammableWeb**

...it continues to be one of the most, you know...

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

Effective ways.

**David Berlind – Editor-in-Chief – ProgrammableWeb**

...susceptible and vulnerable areas of Internet security. Which by the way, that shouldn't be lost on this particular community either because you can imagine a hacker sending an e-mail out that poses to be one of those automated e-mails that comes from a healthcare portal and gets those users to login. I can imagine my father or certainly other users of the Internet who are not quite so savvy about issues, falling prey to that kind of attack. But, I don't know of one other than, you know, I do think the doctor's office represents a great opportunity to educate people who are passing through them.

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

Um hmm.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

And there are also content companies, like ours; this is Leslie again, that provide information and be happy to share that with you, Aaron.

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

Thanks so much, because I think that is the biggest, you know, we can create all kinds of checklists and so forth but the consumer ultimately is the one that is taking the risk and should be making an informed decision. Obviously they have the right to their data in any form they want, but we need to educate them on why APIs are preferred, why other methods might be preferred compared to insecure e-mail and really get their confidence and keep their trust by doing that.

**Shue-Jane Thompson, DPSM, ITIL Exert PMP – Partner, Cyber and Biometrics Service Line – IBM Public Sector**

I think your question is right...would also contend that in addition to just traditional security, you know, privacy type of training, now I think this is the continual learning. The best way to educate our consumer, like I said educated consumer, is the best consumer, that in my orig...not including the blog and webcast and also, you know, I mean...from learning and there are materials available, I am happy to share with you, how we go about that in IBM and also some past lessons learned and how to evaluate whether it's effective and how you continue to evolve your training material, your education material, to ensure that we stay ahead of the curve, if you would, because our world is changing every moment.

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

Do you think that kind of education is something that would be a good function of government? Or, I mean, it doesn't vary by vendor or Good Housekeeping Seal of Approval provider?

**Shue-Jane Thompson, DPSM, ITIL Expert, PMP – Partner, Cyber and Biometrics Service Line – IBM Public Sector**

To my view, I think earlier we were talking about the boundary, right? To see, you know, how does...advance dealing with the healthcare API issues really has to be, you know, all hands on deck. And so this is a partnership and who should be leading education, I think dual, I mean, you know people like, you know...provider like us, we also have the responsibility because we have direct interaction with your consumers and...and even more so, so I think this is...responsibility if you would because we are not just dealing with one type of consumer, we have consumers in many...that is what creates the complexity, if you would agree with me.

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

That makes sense; thank you so much.

**M**

I just want to say that your question mentioned educating consumers about APIs, which I don't think, in my estimation would be a very good idea. If the APIs themselves are in...are essentially in fabric of what we're talking about, it's too low level, in my estimation, it is too much detail to get into; it has to be much simpler.

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

It was almost...(Indiscernible)

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

It's almost like the Schoolhouse Rock version of an API.

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

I was going to say, remember the abstinence, the only way to be sure you don't get pregnant is not...it's just, the only way to be absolutely certain your data will not be breached...

**W**

That wasn't very effective, Aaron.

**Gray Brooks – Senior API Strategist – General Services Administration**

Just to echo that earlier point though, we should always be aware of our ability to be to prescriptive the way that is counter-productive because, you know, government has a very robust ability to do that, and especially in technological areas.

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

...was a comment to?

**Alisoun Moore, MPA, MBA – Senior Director of Corporate Development for the Federal Sector – LexisNexis, Inc.**

I wanted to comment, that was an excellent question and I do think that if you are going to pursue and keep pursuing standardized API with a sort of a seal of approval that some consumer education would be quite useful.

**M**

But I have got to say, it also cuts both ways, it is not just about consumers, the developers should know that they are dealing with an API that has...

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

Everybody, yeah, the whole ecosystem.

**M**

Yup, exactly. Because there is no faster way for an API provider to evolve, you know, and get business...get more business than making sure they get that seal of approval. They don't want to be ostracized as a result of not...from an ecosystem as a result of not having it.

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

Right.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

So, maybe that is an action item is, how we look at...how do we harness the work of white hat hackers in a way that helps this effort? And maybe that is something ONC could look at.

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

Um hmm.

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

Leslie, it looks like you have the next question.

**Leslie Kelly Hall – Senior Vice President of Policy – Healthwise**

I'm good, thanks.

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

Okay. Meg Marshall?

**Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation**

Hi, thanks. So I am trying to piece together and pull together some of the things that we have heard today and I would like to present a couple case scenarios that really kind of drive around the examples of authorized access to data, but unauthorized use of data and just kind of open it up and see if there are, you know, if the panelists have any recommendations around policies we should consider as we look forward...as we hear these types of things.

So one of the use cases is, from a consumer facing perspective, the consumer requests their patient data and unbeknownst to them, the App consuming their data either sells it or contributes it or uses it in a way that they may not have consented to had they known ahead of time.

And then from a provider perspective, one of the issues that we hear is a general concern that the aggregator of the data, so again the App consumer could potentially reverse engineer or aggregate the data to obtain some sort of competitive advantage. So what I am hearing is that this is, again, a little bit of a tight integration. So the API developer, through specifications, through requirements, through terms of use, the consumer through informed, educated activities and then certainly around the Apps client or the App consumer transparency of the data uses; are we missing anything or is there something...am I way off base? I'm just again trying to figure out what other types of policies or questions should we be asking specific to those two use cases?

**David Berlind – Editor-in-Chief – ProgrammableWeb**

One thing I alluded to in my extended written testimony that I did not mention in my oral testimony was that terms of use can also apply to the applications themselves and very often, that is an overlook, that is again a checklist item they often overlook. Now let's be clear, terms of use typically don't prevent a determined hacker from doing something, I mean, they ignore the terms of...generally speaking, they ignore the terms of use.

But, I was very struck by two tests that I ran. First of all, I was reversing...I was using a freely downloadable application to reverse engineer the API for two well-known brands. And the one brand, when I ran their mobile application, which you have to start the application to begin the reverse engineering process, the application had no terms of use on it whatsoever. So, there was no, I am not sure that that the...that that brand, that company would have any legal recourse as a result of the, not only the reverse engineering I did, but the toying around with the API that I engaged in after that.

On the other hand, another organization and I can tell you this one because I didn't go any further, right? The NHL, and this example is in my written testimony, has a splash terms of service that confronts you when you first launch the application, before you can go any further, that has very clear language about things like reverse engineering it, circumventing controls and security, etcetera.

And again, I don't know that terms of service are going to prevent hackers who are determined to do whatever it is they maliciously choose to do. However, and I am not a lawyer, but my guess is that those terms do create a little more of a legal remedy and recourse in the event that somebody malicious is caught doing something like that. And they have to recognize that the application itself essentially to hackers represents an entry point into the API. And so maybe those terms of service, again as a best practice, a checklist item, should universally apply to the application as well as the APIs. And my written testimony shows a screenshot of the NHL's application and the very clear language.

**Alisoun Moore, MPA, MBA – Senior Director of Corporate Development for the Federal Sector – LexisNexis, Inc.**

This is Alisoun again from Lexis. We almost always have very clear data usage language in our connections to clients through our API and I would strongly urge that that be part of it. With a lot of the Facebook and other services like that, what a lot of consumers don't quite understand is who gets access to the information they are posting and that information is used for commercial purposes. So if you are going to protect the consumer's information, the patient's information and also protect

providers who are covered entities under HIPPA, you would have to fully disclose exactly how their information would be used, so that they understand what the risks are when these that API.

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

Okay. Well, hearing silence, we don't have any more questions in the queue. So let me first just check and make sure the task force members don't have any more questions. Okay, well it seems like we will be able to wrap up a little early today.

So let me first, before we wrap up, turn it over to Meg and Josh to make a few concluding comments and then we will open it up to public comment.

**Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

All right, thanks Michelle. And before we launch into closing comments, actually we wanted to just briefly call on Lucia Savage at the Office for Civil Rights, because there was a question that came up about the notion of data ownership and I just wanted to make sure that we got the record straight on what the official story is when it comes to ownership of healthcare data; so Lucia, if you are on the phone, this would be the perfect time to have you comment.

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)**

Lucia with the ONC.

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

Yes. We do have Linda Sanches on as well, she was on at the start of the call.

**Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services**

Hi, this is Linda Sanches; I am on the call. Speaking from OCR, I can't really address data ownership questions, but people brought up many other areas of concern and I am happy to work with ONC and the committee members to listen to the play out what some of the cases, use cases are of concern so we can see if there is guidance that you might be needing.

**Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology**

Hey Linda, this Jeremy Maxwell from ONC; could you also take a second to speak to some of the patient access guidance that you guys have recently released because I think that is very applicable here.

**Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services**

Okay. Well, and I think this may have been alluded to earlier by one of your speakers, we did recently publish and post on our website some updated guidance regarding the access provision under the Privacy Rule. Under the Privacy Rule, people do have the right to obtain from covered entities and their business associates, copies of their records and the right to access those records, and I am speaking very broadly here.

This has not changed, but we did decide it made sense to put out some updated guidance because there continues to be a struggle in the industry with actually needing this, right? So we did put out some new

statements and explanations of the access rights and also put out a series of questions and answers around how it works. So I really encourage you all to take a look at that. There are additional areas that we will be publishing in the coming months, for instance around what is an acceptable fee for the work of producing it, but there are, I think it is like 30 pages of Q&A to help people think through how to honor the access rules and make sure people do get access to what they need.

**Rose-Marie Nsahlai – Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology**

Thanks, Linda. This is Rose-Marie from ONC; I know where planning on reaching out to Michelle to see the access guidance that will be helpful to our panelists as well as to our task force so we can disseminate that information out so they can have more awareness. I know Lucia also referenced the issue of data ownership; it is a state law issue so she was also planning to have that included on some of our analysis and final report that our team will be doing internal at ONC. So hopefully we will be able to send our more information to the panelists, as well as to our task force on data ownership questions.

Lucia, I don't know if you were able to join, but I know she has been actively listening in and we have been chatting quite a bit. So Lucia? Okay, well I will follow-up with Lucia and will make sure those items are addressed, thanks.

**Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Department of Health & Human Services**

Yes and I will definitely pull together some points for the panel on the access guidance.

**Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

Great; thank you very much. So at this point, we are going to wrap up with some brief closing remarks. First off, I want to thank the panelists from both of our panels for their testimony and also for their time in putting it together and delivering it. We recognize this is no small investment, but we really appreciate it and we are looking forward to synthesizing all that we have learned today and what we will learn later in the week in our second round of testimony and putting together some recommendations based on all of this.

So to briefly summarize the first panel, we heard from a set of consumer facing companies that have been deeply involved in the API economy. We heard from a team working on the Green Button effort, which in a lot of ways was inspired by, but has grown out of the blue button community to provide consumers with access to their energy data. It acts as sort of an alternate universe for us when we think about using very similar principles to supply consumers with access to healthcare data, and we can sort of see what the future looks like through that lens.

We heard about the importance of creating an engineering culture where security is a first priority and where the culture can grow with the ecosystem and push forward the state-of-the-art and adapt new best practices as they emerge and actually shut down the old practices when they are no longer considered best practices. And we learned that just because a system is buzzword compliant and standards-enabled does not always mean that it is more secure a real-world and a practical sense.

We talked about API gateways as one best practice where you can apply a set of conditions up front, things like rate limiting and audit logging that can be applied at one consistent entry point into a series of APIs.

We talked about how important it is to allow users to express their preferences for sharing in rich ways including letting people make decisions, but also letting people take back those decisions. Letting users make decisions ahead of time rather than being forced to make a decision on the spot at the time when an App or someone else wants to get access to their data.

And during our discussion, we talked through a lot of the real-world experience that companies have had in exposing APIs both inside and outside of healthcare for applications that are connecting to data for consumers today. Including ecosystems where consumers can bring their own App to the table and there is not a detailed or a heavy process by which Apps are vetted ahead of time and consumers get to make those decisions about which tools they want to use.

So again, thanks for the rich discussion in that first panel and let me turn it over to Meg for a brief summary of the second panel.

**Meg Marshall, JD – Director, Government Health Policy – Cerner Corporation**

Thanks, Josh and again, thanks to both panelists; what a fantastic day. So on panel two, we also heard from consumer technologies; we heard from experts at LexisNexis, US Digital Service, ProgrammableWeb, Oracle, General Services Administration, and IBM.

And I may not be able to capture as well as what Josh did, but we walked quite a bit around organizations that use APIs for Apps available externally to third parties, the processes for making available...documentation available throughout that process.

We talked quite a bit around consumer protection and the concept of that and how important it is and introduced a seal of approval or certainly some sort of requirements for a checklist. We discussed standardization of APIs activities to support white hat activities and other types of concerns around allowing large sets of unknown developers' access to protected data.

And we did have some thoughts around some of the privacy and ownership and we expect to hear back from OCR and other individuals that HHS around that. Josh, I know I missed a huge...I wrote until my fingers cramped up and then...on my computer, so, anything that I missed?

**Joshua C. Mandel, MD, SB – Research Faculty – Harvard Medical School**

No, I think that was a great summary from my perspective.

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

Okay, well thank you both, Josh and Meg and thank you again to all of our panelists. We do have another virtual hearing coming up on Thursday. So let's open up public comments and see if there are any public commenters; Lonnie or Jaclyn?

**Public Comment**

**Lonnie Moore – Virtual Meetings Specialist – 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 the telephone and would like to make a public comment, please press \*1 at this time. Thank you.

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

While we wait to see if there is any public comment, if you would like to submit a written public comment, there is an e-mail address up on the screen, it is [fac-a-onc@altarum.org](mailto:fac-a-onc@altarum.org), if you want to send any written public comment. And you can also put a public comment in the chat, which appears below, on the screen. And it looks like we have no public comment.

So thank you again to all of our panelists, thank you to all of our task force members to the rich discussion that we had today. We greatly appreciate everyone sharing their expertise and you spending your time with us today and we look forward to the next hearing on Thursday. Thank you everyone.

**Public Comment Received During the Meeting**

1. John Moehrke: The best approach I have seen to changing development/deployment culture is the "Privacy By Design" initiative. GE Healthcare has adopted this a few years back.

Meeting Attendance				
Name	01/26/16	01/12/16	12/04/15	11/30/15
Aaron Miri	X	X	X	X
Aaron Seib	X		X	X
David Yakimischak	X	X	X	X
Drew Schiller	X	X	X	X
Ivor Horn	X	X	X	X
Josh C. Mandel	X	X	X	X
Leslie Kelly Hall	X	X	X	X
Linda Sanches	X	X		X
Meg Marshall	X	X	X	X
Rajiv B. Kumar	X	X		
Richard Loomis	X	X	X	X
Robert Jarrin		X	X	X
Rose-Marie Nsahlai	X	X	X	X