

Health IT Joint Committee Collaboration

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



Joint Health IT Policy and Standards Committee Application Program Interface Task Force Virtual Hearing Transcript January 28, 2016

Presentation

Operator

All lines are now bridged.

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

Thank you, good morning everyone this is Michelle Consolazio with the Office of the National Coordinator. This is a Joint meeting of the Health IT Policy Committee 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 meeting. As a reminder, please state your name before speaking as this meeting is being transcribed and recorded. And I will now take roll. Meg Marshall?

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

I'm here.

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

Hi, Meg. Josh Mandel?

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

I'm here. Hi, Michelle.

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

I'm here, good morning.

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

Hi, Aaron. Aaron Seib?

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

Here.

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

Hi, Aaron. David Yak?

David Yakimischak, MBA – Senior Vice President & Chief Quality Officer – Surescripts

I'm here.

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

Hi, David. Drew Schiller?

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

Yes, here.

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

I'm on.

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

Hi.

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

Good morning, it's Rajiv.

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

Good morning. Richard Loomis?

Richard Loomis, MD, CPC – Senior Medical Director & Informatics Physician – Practice Fusion

Hi, good morning.

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

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

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.

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

Good morning.

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

Anyone else from ONC on the line?

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

Hi, Michelle, this is Jeremy Maxwell.

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

Hi, Jeremy, thanks for joining. Okay, well thank you all, thanks for joining our second part of our two virtual hearings. I just want to go over...

Steven Keating – Patient Advocate/Consumer – Doctoral Candidate, Mechanical Engineering, MIT Media Labs

I just wanted to check in, I'm here, Steven Keating.

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

Hi, Steven.

Steven Keating – Patient Advocate/Consumer – Doctoral Candidate, Mechanical Engineering, MIT Media Labs

Thanks.

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

Thanks, for joining. So, I just want to go over a few administrative items again for our Task Force members and for our panelists and then I will turn it over to Meg and Josh. So, just a reminder, again, to our Task Force members when we open it up to the panelists questions please put yourself in the queue by using the hand-raising feature.

And, again, the questions that were sent over to our panelists are on the second page of the agenda if you want to take a look at that.

And just a reminder to all of our panelists please try and stay as close to five minutes as possible. I will ask you to wrap things up if you start to exceed your five minutes and I appreciate your patience with me in advance and with that I will turn it over to Josh and Meg.

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

Thanks, Michelle and welcome everyone. I think we'll keep the introductory remarks brief because I know we have a lot of exciting testimony and then discussion ahead of us but I just want to say thank you especially to all the panelists for joining. This is our second and final day of public hearings as part of the API Task Force.

In the first meeting that we had, earlier this week, on Tuesday we heard from a group of consumer-facing health technology companies. We learned a lot about some of the security and privacy considerations involved in real-world deployment of services both outside of the healthcare space and a little bit touching on sensitive data especially and looking forward to hearing today from folks closer to the inside of the healthcare delivery space.

So, we've got three great panels lined up with a focus on healthcare delivery on health IT vendors and then finally on consumer advocates. I will refer everyone who is listening to the agenda for a list of the questions that were asked to the panelists because we don't give the panelists very long to provide their responses and many panelists won't have time to reiterate all the questions in their testimony so for reference at the bottom of the agenda, as Michelle said, there is a set of questions that we asked and they're slightly different questions for each of the three panels that we'll be hearing from this afternoon. So, with that I'll ask briefly whether Meg has additional introductory remarks and then we'll kick-off panel number three.

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

Thanks, Josh. I just wanted to echo the thanks to our panelists for your time and expertise and also to add a thank you to the ONC staff. A lot of behind the scenes work went into enable this opportunity and we really...we do appreciate that. So, thanks to everyone.

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

Thanks, Meg. Okay, so we'll get started with Panel three. I just want to do a quick check and make sure that all of our Panel three panelists are on the phone I think we might be missing one person who we'll move to the end. So, I know Stan Huff is on. Is Paul Matthews on?

Paul Matthews – Chief Technology Officer – Oregon Community Health Information Network

Yes, I'm here.

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

Hi, Paul. Is Sean Kelly on?

Sean Kelly, MD, FACEP – Chief Medical Officer – Imprivata

Yes, I'm here.

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

Hi, Sean. Tim McKay?

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

Yes.

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

Yes, I heard you. And Brian Lucas you're on as well? Okay, so we have everyone. All righty, so with that we'll kick-off with Stan Huff from Intermountain and whenever you're ready Stan. Ut-oh, did we lose Stan?

Stanley M. Huff, MD, FACMI – Chief Medical Informatics Officer – Intermountain Healthcare

I'm on mute, now I'm...sorry. So, I'll just tell a story about what we're doing basically and then hopefully we can have some goods discussion and questions.

Intermountain has been interested for a long time in standards-based services and we've worked internally with formal representations of information models and terminology to accommodate that and then we've been very active in HL7 and in the CIMI modeling activity, and in the Healthcare Services Platform Consortium. All of that can probably be summarized best by saying that we've been strongly committed to the FHIR strategy from HL7 and to the SMART strategy for integration of applications into EHR systems.

And so, we negotiated with Cerner when we contracted to begin using their system with Intermountain Healthcare that Cerner would support not only for us but their other customers standards-based services and then subsequent to the contract we decided that the APIs that we would standardize would be the FHIR APIs and, you know, we've worked then to develop with Cerner the FHIR-based services. They actually program the services but we decide jointly the specification of those services and, you know, what terminology we'll use and what information models we will use inside of the FHIR framework.

And so we have active projects going on. We have one application that we actually borrowed from Boston Children's Hospital from Josh and others on his team as a SMART on FHIR application that's a pediatric growth chart application. We have that live now in our production system in a parallel mode. It's not used by everyone right now but it's used live by a set of people in our pediatric intensive care unit.

So, yeah, you know, we're supporting standard APIs. I mean, it's very important to us that we're using those standard APIs rather than the proprietary interfaces that Cerner has had for a long time in their millennial objects.

We continue to use their...you know Cerner's proprietary things too because we don't have enough infrastructure in place that we could do all of our new development against the FHIR services yet and a lot of the services are still under development but we've got that application. We've also got...we've got other applications that are in development, a pulmonary embolus application and IHE viewer application that's in production.

And then internally we're using the same APIs to make access to our legacy systems so that we can standardize the interface to that data and we can transition that data from...and keep that data available through those standard interfaces moving forward. So there are a lot of internal resources that are focused on using the FHIR APIs internally as well as for these, what we hope will be shared, open applications.

So, that probably gives you enough context at least and I'll stop there and then, you know, we can take questions and have further discussion about particular points people might be interested in.

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

Thank you, Stan, sorry.

Stanley M. Huff, MD, FACMI – Chief Medical Informatics Officer – Intermountain Healthcare

That's okay.

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

Paul Matthews if you're ready?

Paul Matthews – Chief Technology Officer – Oregon Community Health Information Network

Yes, hi, good morning, this is Paul Matthews I'm the Technology Officer at OCHIN. I'd like to thank the Task Force for the opportunity to share our experiences with you on APIs in the healthcare ecosystem.

And when we look at OCHIN, OCHIN is health center controlled network serving 90 organizations across 18 states and we provide services for about 4700 providers. We also act as the Regional Extension Center within Oregon and so part of our testimony is looking at this from an ecosystem from the small provider practices not just from the larger organizations.

Our members include federally qualified health centers, FQHC work lookalikes, rural health, behavioral health, school-based health centers and county health departments and with that we have a large number of requirements and requests to share information that requires us to look at APIs sometimes in a different way.

Healthcare organizations and health IT vendors are gaining and understanding that APIs, if structured correctly, can foster innovation and increase availability of market-driven Apps. And when we look at those application lists we're thinking more about mobile applications for the mHealth Initiatives and we're thinking about research. How do we get information into large data warehousing to do research? And especially we run a practice-based research organization and we'd like to look at that information in ways, from those small practices, to provide better outcomes within those patient communities.

I think a recent Harvard Business Review article, The Untapped Potential of Healthcare APIs, by Robert Huckman and Maya Uppaluru, raised four key points and I think those key points are very well stated in their article and we'll add to it a little bit.

The first point was financial incentives for providers need to encourage the data exchange necessary to deliver better outcomes. And at OCHIN we see this actually happening as we move away from a fee-for-service-based model to value-based payments and we have a large amount of work occurring in Oregon on value-based patient payment initiatives and especially around CCOs within Oregon, ACOs for the rest of the country. The pressure is already beginning from those Accountable Care Organizations but it's only going to increase and accelerate through MACRA payment models.

The second point they raise were concerns of patients and providers around privacy and security and while the article...they suggest two key standards, OAuth and OpenID, for security and authentication. I think that the issue that we see is small provider practices have an extreme reliance on their EHR vendors to understand what that means from a compliant stand-point and what this represents from an implementation and a risk mitigation need. And so these small practices tend to rely so heavily that they will actually allow the vendors to suggest specific standards to them without understanding what that means.

And so there's a lot of translational work and training, and education that needs to occur and I think the Task Force can help us in suggesting ways for creating a translational knowledge bridge that says what does the standard actually mean? What does this suggest to you from compliance terms? And what are the compliance options that come up for a small practice?

The third point they raise is vendors should implement open standard APIs with transparent terms of use, policies and developer fees. And we've seen an environment change to value-based payment and data movement analytics and reporting requirements are increasing and it's imperative that the healthcare organizations and especially the small practices understand those terms of use and specifically the cost for utilization and maintenance of those APIs.

Frequently we see APIs modified, especially when we saw these in the HL7 fields, the use of z-segments with inside of those solutions that allowed organizations to create variance in such a way that the implementation to multiple organizations or payers, or laboratory systems has increased the cost dramatically for those small providers removing their ability to necessarily shop for best services because the cost of movement has become extremely high.

The second...the last one, the one, point four that they raised is the cultural and workflow issues within healthcare systems. Moving a culture within an organization is difficult but it can be overcome if you show rapid development and value to your community or to the practice themselves. And in the current environments the propriety APIs that we see in use today and the modification that occurs on those is actually providing a large gap in the value of the data.

We see numerous implementations where current standards and regulations specify specific vocabularies and in those suggestions we find gaps sometimes upwards of 30% of the data and the value in the data. They're missing the coding and this is going to increase frustration across the developer community because they're going to have to do large mapping and data mapping projects to match information from the data they receive to the data that they want to display to the patient or the user.

And so it's very important we look at standardized APIs, standardized coding and standardized vocabulary with inside of that information. The data value is the most difficult piece. The transport, the authentication is not the technical difficult component of this.

So, in conclusion, I'd like to say that OCHIN supports the Task Force work on open APIs. We would reinforce that when looking at implementation of APIs we see this as evolutionary and not a revolutionary stance.

An API should not allow for variance in the basic implementation requirements such as those in the z-segments of HL7, but we should look at extensions added to the APIs and not require them to be supported and this will allow functionality within organizations to be standardized and developers to actually create tools that are useful and agnostic to the EHRs they're communicating with and I'd like to thank you for your time and we'll wait for the questions.

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

Thank you, Paul. Sean Kelly?

Sean Kelly, MD, FACEP – Chief Medical Officer – Imprivata

Yeah, thanks, Michelle, and thank you, Josh and Meg for the opportunity to testify today before the Task Force. Imprivata is a healthcare IT company that provides authentication access management and identity solutions for healthcare. Our mission is essentially to make security convenient.

I wear several hats, I'm the Chief Medical Officer for Imprivata and have doing that for about four years, but I'm also a practicing emergency physician in Boston, Massachusetts. It's really through that lens today that I think will be most helpful for me to speak with you and give my perspective as a provider. As such I strongly advocate for open frameworks that improve interoperability and access to patient data.

Medically, ethically and legally access to data has a very significant impact on care delivery on a daily basis. For example, later tonight if I'm on duty in the ER, 2 a.m. in the morning, and a comatose patient arrives in the ER it's really essential for me to access their protected health information as quickly and securely as possible. I need to know many things really as soon as possible such as what is their medical history, do they have allergies to medications, any recent trauma, are they on anticoagulants, insulin, other medicines, what's their code status, do they have advanced directives, do they have a healthcare proxy? You can imagine all these things have a very significant effect on the care that we can deliver.

And it's really not an exaggeration to say that having immediate access to this pertinent data can be lifesaving. It really directly affects patient safety and outcomes of care I think we all inherently understand this.

You know in fact, access to data is so important to me as a provider that even if this were to require complex processes to be allowed to access it, such as supervised enrollment, credentialing or access controls or strong authentication methods, it would still be preferable to go through that then to not be able to access that same patient information when we need it most and good technology can actually reduce the complexity of such security standards allowing for convenience and efficiency in addition to security if implemented properly that's of course what this discussion is about.

You know I feel that this type architecture already exists certainly in many other industries such as the financial and criminal justice systems. We've seen other industries pave the way on APIs and other such technologies so far.

You know I would not, of course, recommend ignoring the risks involved in streamlining access to patient records through such technology, however, there really are effective ways to mitigate these risks. In fact you don't have to look beyond healthcare the precedent has already been set within this industry for such a system.

Technology solutions for things such as electronic prescription and controlled substances demonstrate how supervised enrollment procedures, strong authentication methodology, including biometrics, can be used to comply with even the strictest security standards such as those set by the DEA in their interim ruling and this can be done conveniently and securely if done properly as has been discussed in prior committee meetings and I'm sure will be discussed today.

In short, there are really already proven methods in the healthcare industry and beyond that we feel facilitate the secure exchange of potentially lifesaving data while still mitigating the risk of sharing that data.

And really the major point that I would like to convey as a provider today is that the risks of such interoperability are far outweighed by the risks inherent in not sharing essential data between caregivers as too often happens right now today in the status quo.

Most healthcare professionals I think would support a standardized architecture allowing for exchange of data even if it did require enrollment ahead of time, strong authentication methods such as biometrics, you know, I went through personally just such a process just to get my global entry card so I could go through TSA more rapidly, I certainly wouldn't mind doing it to help serve my patients and comply with the Hippocratic Oath, which as you know states first "do no harm."

So, I think that most providers and technology vendors would support open access to data if done correctly. I thank you for inviting me to testify today. I look forward to the questions and hopefully a very, very good discussion. Thank you.

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

Thanks, Sean. Tim McKay?

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

Yes, thank you. Co-Chairs and members of the Task Force my name is Tim McKay, I'm the Senior Director of IT Product Management and Delivery at Kaiser Permanente, which is the largest private integrated healthcare delivery system in the United States. And before continuing on behalf of KP and the National Cybersecurity Alliance I'd like wish you all a Happy National Data Privacy Day. And note that our testimony documentation will be submitted after today's hearing.

Since 1994 I have led Internet development projects for Kaiser Permanente. Currently, I manage a project portfolio focused on designing consumer-facing health IT products for kp.org our patient portal which has over 5 million active consumer accounts. And through kp.org consumers can access their

medical records, manage prescriptions, locate services, schedule medical appointments, pay for services and access health and wellness resources.

During Tuesday's hearing you heard from App developers and vendors how utilizing API enabled capabilities are effective and in wide use to access publically available information such as National Weather Service data. Today, I'd like to expand on this theme and discuss security, privacy and operational concerns when considering accessing personal health information through APIs.

Kaiser Permanente believes that API technologies have tremendous potential to help consumers manage their health. In 2013 we launched our core API program named "Interchange" by Kaiser Permanente.

Interchange allows third-party developers, Apps and devices to securely use KP provider, facility and location information for 38 hospitals and more than 600 medical offices. Our API program documentation is available online via our Interchange portal at developer.kp.org. We also include a sandbox for testing Apps against our data as well as technical guidelines and FAQs. Developers must register with Interchange to interact with the system.

Interchange is not yet enabled for accessing patient specific health information. While our API program supports OAuth 2.0 for authentication and authorization of Apps and devices we strongly believe that a critical first step will be to develop a comprehensive ecosystem and infrastructure to ensure access to patient's clinical information is full secured.

Our main concerns encompass the following issues, first, the potentially large volume and variety of Apps and devices attempting to interact with EHR systems will make App and device identification, validation, verification and overall management very complex as it is important to know how any specific App or device would interact with the unique characteristics and requirements of any organization's data systems.

Consideration should be given to establishing a trusted source for certifying Apps and devices so healthcare organizations do not have to develop independent programs for App security, privacy and compliance certification.

Second, App and device authentication and authorization mechanisms that purport to act on behalf of the patient have not been fully proven. And the appropriate level of access to specific patient health information for Apps and devices has not yet been well defined in either a policy or technical capability context.

With healthcare cybersecurity concerns at their highest level ensuring that only properly identified, verified and authenticated Apps and devices are authorized to enter an EHR system to access and extract patient health information is a significant and an overarching challenge.

From the security perspective for instance, it might not be sufficient that the App or device knows the patient username and password and a token-based key-driven approach to authentication and authorization would require a national ecosystem with trusted issuers and cross validation of keys to be effective.

Third, establishing and maintaining a common industry standard for detailed sets of audit logs to document attempted and successful access changes in extractions of health information will be crucial for protecting data privacy.

And last, it would be helpful to assess whether and how other regulated industries address App and API interactions with core basic datasets. For example, has the financial services industry considered supporting the use of personal Apps for accessing consumer bank accounts as an alternative to bank supplied Apps?

Keeping patient information private and secure consistent with federal and state laws and consumer privacy choices is a top priority for Kaiser Permanente. We believe API technologies are already beginning to impact how consumers interact with healthcare organizations.

However, we believe these technologies will still need to evolve to a point of maturity that will allow healthcare organizations and consumers to use them appropriately, confidently and securely. Until that point regulations requiring their adoption and use would be premature.

I thank you again for the opportunity to participate in this hearing and look forward to discussing some of these points with the group during the Q&A portion of the session.

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

Thank you, Tim. Brian Lucas?

Brian K. Lucas – Enterprise Systems Architect - Aetna

Good morning, how are you doing today? I will be speaking to the slides that are included in the materials so if you want to follow along on those slides that might be helpful. First of all, thank you for the opportunity to speak to you today about what we consider to be an important discussion on API privacy and security. We see APIs as the key mechanism for participating in digital healthcare ecosystems and our opening slide sort of illustrates that.

The two goals we believe need to be met are making APIs easy to use for the developer but also safe for the owner of the information and the business processes that are exposed. So, this dual focus open and safe form the basis for our opening remarks today. We're going to touch on three areas.

We'll do a short overview of our view of APIs and their roles in the digital ecosystem. We'll look at the current state of APIs at Aetna and some going forward concerns for open and safe deployment of healthcare related APIs.

Aetna really sees our mission as building a healthier world and there are three primary focuses for this business that we're in. We want to create healthier communities, a healthier nation and a healthier world. We want to help individuals be healthier as well. We see this happening through aligned economic incentives that address affordability of healthcare and digital strategies that enable a simpler, more transparent consumer experience by deploying technologies that can seamlessly connect to our health systems. We believe that open secure APIs are a key component of engaging the healthcare ecosystem to build a healthier world.

We think that this move to APIs is also driven by changes in our business drivers. The business drivers in the United States healthcare system are shifting focus. They are shifting from our cost and delivery of care from our old fee-for-service where providers are reimbursed for providing services to value and outcome-based reimbursements where providers are...reimbursements are linked with quality of care.

We also see consumer experience expectation shifting from what were primarily employee centric and low tech to consumer empowered technology enabled solutions. Administration and services are also shifting from complex internal systems to online distributed self-service systems and the industry focus, in general, we believe is shifting from the needs of those who pay for the care to the needs of those to access healthcare. These shifts combine to broaden the number of players in the healthcare ecosystem and the need to share our data openly and securely so that we can meet these evolving expectations of a new healthcare ecosystem.

Moving on to Aetna's current state. We're about five years into our API journey. We began our journey in 2011 exposing APIs that access healthcare information and perform healthcare related functions. We started small, incorporated lessons learned and continue to deepen and broaden our enterprise API support.

We have also versioned APIs and deprecated older APIs to keep up with the evolving needs of the healthcare ecosystem but also intend to support different forms of APIs using the same underlying information. The APIs that we have in production use today are used by mobile, web, voice and business partner applications both internally to Aetna's ecosystem and externally.

Our users include clinicians, customer service representatives, providers, consumers, brokers just to mention a few of the consumers of our applications. Some of these applications are built solely using our API set and some combine new APIs with other interface mechanisms like older SOAP services or file feeds to meet their local needs.

Today, Aetna continues to manually grant access and distribute API documentation, such as developer guides and API documentation, to parties who are interested but also vetted. Before consumers are granted access to APIs they must pass our security and privacy assessments and possibly scans, and agreed to terms of use that are appropriate to the level of access that they request.

Our roadmap includes exposing API documentation to registered development communities also commensurate with their vetted level security and privacy policies and technologies. Our APIs are managed with industry-standard security and privacy tools, policies and procedures to make sure that the underlying information and capabilities are secure and auditable.

Going forward I think we share many of the same concerns we've heard from other folks today. Because the US healthcare industry is highly regulated and complex and because constituent expectations for protecting their personal information are high one of the biggest areas of API focus is also a paradox.

How do we encourage open and seamless sharing of healthcare information and capabilities while still fiercely protecting the security and privacy of the information that we are entrusted with? Existing and emerging technologies such as Open Authorization Framework 2.0, device signatures, OpenID technologies like that must be integrated into API solutions to meet regulatory requirements and constituent expectations yet remain easy enough for developers to consume on their mission to advance healthcare interoperability.

Our strategy also includes continuous improvement to our API offerings. API development is a long-term capability and we believe APIs should be grown over time, provide additional levels of security and coexist gracefully with existing interface mechanisms. This allows an organization, as well as the entire industry, to securely yet quickly advance the healthcare ecosystem by leveraging existing technology in newer, more lightweight and easier to consume ways.

That concludes my opening comments. Thank you, again, for the opportunity to present this short overview of Aetna's API experience and strategies.

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

Thank you, Brian, and thank you to all of our panelists on Panel 3 we greatly appreciate you sharing your insights with us. I will now turn it over to the Task Force to see if there are any questions. It looks like Leslie Kelly Hall has a question.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Thank you, thank you that was really insightful and bravo to you all who have moved in the direction of using APIs for healthcare. I think that your cautions are well noted but the opportunities seem terrific.

I have a couple of questions, one for I think Tim, you mentioned both a single body potentially to provide either a Good Housekeeping Seal or somewhere house APIs for healthcare and then talked briefly about how it also still needed to be open and I wondered if you could talk a little bit more about that idea?

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

Sure, so, currently for example at HL7 the Mobile Health Workgroup is working on a standard for consumer mobile health applications and the intent of the standard is to address the security, privacy and data concerns and so that potentially there would be a framework for certifying health Apps against which could at least provide a first level of work against compliance issues.

What...the concern, generally that we have is how open of an API system are we are looking at? Are we looking at first a set of approved and curated Apps that would be able to access the system that we have a high degree of insurance that at least there has been sufficient consumer notice about data uses that security and privacy constraints and controls are being addressed appropriately versus a completely open where anyone could bring their App of choice to access data from the system.

That gets more concerning when we just try to look at how we maintain our security controls and how we make sure that the App itself isn't doing something digressive in terms of using data in a way that perhaps a consumer agreed to in the terms of use but there has not been transparency really with how the data is being used through secondary workflows.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Great, thank you, so you're suggesting that there are bodies already emerging that have the ability to give a framework for certification.

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

Yes.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

And that's a good first step but there may need to be ongoing either standards or governance structure that supports this. Did I hear that correctly?

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

Yeah, I think so. In part...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Okay.

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

Part of what I think the standard at HL7 was meant to be progressive in terms of dealing with the very low hanging fruit to begin with such as making sure that terms of use are being constructed correctly, that people have the ability to review privacy policies, that use of certain device capabilities and authorization to send data, extract data or send data to various sources is very clearly explained within workflows rather than embedded in terms of use but that will get you so far.

Ultimately, though you really need to take a look at the specific App from more of an engineering point-of-view to make sure that the App is playing well with your system, that there isn't anything that is going on inadvertently.

So, think of the HL7 standard first of providing a sieve at a high level as filtering out egregious types of Apps with very poor data security and privacy controls. But, again, at least the state of...that we're anticipating that this standard will be over the next few years is it will knock it down to necessarily the granular level that you would need for certifying against a particular system.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Thank you.

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

Stan Huff did you have a comment?

Stanley M. Huff, MD, FACMI – Chief Medical Informatics Officer – Intermountain Healthcare

I do. I just wanted to be sure that we're using terminology in the same way around "open APIs." There are at least two ways that I could interpret that, one is, we have different companies and organizations that are creating APIs and they're making those available and openly publishing them but they're different, you know, for each group, you know, Intermountain could have it's set of APIs, which we actually do, and, you know, companies like Cerner and EPIC could have their own and they do, you know, Cerner had millennial objects and EPIC has it's complimentary set of those and those "open" and they're published and they're free in a sense but that's what exists today and I hope what this committee is talking about is what I would call open standard APIs because what we really want and

what would really provide the greatest benefit to the country is that I can talk to anybody's system in a standard way. And so it's not a bad thing that APIs exist the way they do today that's better than not having APIs and it's, you know, better to have some kind of access.

But to really get the benefit that we want in terms of population health and sharing across organization I need to be able to talk to an EPIC system or a Cerner system or any of Intermountain's legacy systems through exactly the same interface using exactly the same codes and information structure.

And so I guess I would make the distinction between "open APIs" which if people are publishing and making them available you could argue were open and that's probably an appropriate phrase, but open standard APIs says I'm supporting, in this case for instance, FHIR with a very explicitly known set of profiles so that I can talk to any system in exactly the same way and I just want to make sure that we're seeing the difference between those two situations.

I'm very supportive, I mean, incredibly supportive of truly standardized open APIs and I hope that's what the focus is of what we're talking about here.

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

Well, Josh you have the next question and I'm not sure if you want to comment on Stan's comment at all?

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

Sure, what I'll say is, just on a personal level, well, first of all, thank you very much to the panel for their testimony. I can see already there's a lot of questions I've got and I'm looking forward to the continuing discussion.

Just to share some quick feedback with Stan's comments on a personal level, I mean, I agree and I'm spending a lot of my time and effort working toward open standard APIs but I would encourage, for the purposes of our discussion here, if we can focus on the security and privacy aspects rather than the notion of the data payloads themselves. I think that will help us to collect the most relevant testimony for this Task Force.

Because for this Task Force we've left out of scope the issue of what the APIs are and how the data and all the vocabularies work. These are obviously incredibly important issues but they're just not the mandate of our Task Force.

So, the more that we can focus in today's discussion on the security and the privacy pieces the more helpful it will be for us as we come to synthesize the recommendations downstream. So, don't let that discourage you from sharing your thoughts across the board but just so you know where we'll be able to really harvest these discussions later on to bring recommendations back.

I did have a few questions but let me start off with one which is for healthcare provider organizations I would love if any of the panelists would share thoughts about the ideal way to figure out which Apps you're willing to allow to run within a given system and especially if the answer is different for patient-facing Apps versus provider-facing Apps.

And so, you know, for example, how do you make the decision? Is it totally open and just let the users decide what App they want to run? Is it a decision that healthcare provider organizations should be making on behalf of those users or is it something that healthcare provider organizations would rather outsource to some kind of third-party who certifies or approves Apps or some mixture of the above? But I'd love thoughts in the general set of questions.

Stanley M. Huff, MD, FACMI – Chief Medical Informatics Officer – Intermountain Healthcare

So, this is Stan, I mean, what I've...and we're not doing this yet so this is sort of, you know, how we hope the future will be, that there would be certifying bodies that essentially are certifying compliance to the standards, you know, and then there would also then be the opportunity to certify a given App against a given platform.

So, in our case we would want to be able to go on it and it would probably be up to us in a relationship with our vendor to say here is an App that we want to use could you test that to make sure that it's not going to cause performance problems or, you know, somehow disrupt the database that sort of thing, so they're essentially certifying that it acts well in the environment where we're actually going to deploy it.

And then the other part of that though is to say, we really want to keep the prerogative of what applications we want to run and we want to...we think it's our job, as clinicians, to say whether this is an effective App whether it actually does what it does. So, we don't think it's Cerner's job to decide "oh, this App gives bad advice" or "we don't like the user interface" or something else. We think that's our prerogative.

And so, yeah, we want to test against standards and, you know, things like...and I'm thinking of like what the Argonauts are doing and, you know, that's not set up to be a long-standing institution yet, but, you know, some authoritative body that can say this App claims to be conformant to this set of standards and yes we found in testing that it is testing by vendors and suppliers of platforms and applications that say, yes, this application or this service actually runs and is also safe in terms of security and reliability of the system. And then we want to make the determination of whether it's a good App and does what it should and meets our needs.

Paul Matthews – Chief Technology Officer – Oregon Community Health Information Network

Hi, this is Paul Matthews from OCHIN, while I agree with a number of those comments I think the question also comes down to is we have to look at small provider communities and the smaller...and their ability to pay for somebody to do that testing of each of those applications.

And I look at things and say if I remove the compliance side altogether and it wasn't a discussion and we looked at it purely from a technical and engineering exercise I think the questions and the responses I heard so far are very on point.

If we look at the engineering side and say what is the scale of the solution, what are the issues we may face where it would bring errant queries or errant calls into our API that bring our systems to their knees what is the quantity of the data that's going to be moved and is there a...and who pays for that?

Because a lot of the small practices out there will not have the ability to implement to scale for their practices for all the calls that may come into them for data, especially if we look at truly open standard APIs with an ecosystem of applications that are certified and can call into those APIs.

So, if we then layer on top of that the compliance requirements we know from an engineering solution, hopefully, and then we've got on their the compliance issues, I often see the compliance issues being as a way of...gets in the way of the discussion of the technical need and I think that what we need to look at on the compliance side is, are we applying standard understanding to the compliance needs?

Often people go out into the community and will survey the patients about their data and the access to their information and more often than not there aren't concerns at the patient level about the access to that information. And I'm wondering if we've actually conducted a larger survey. I know in Oregon they conducted one a number of years ago where they didn't find issues with access to that information in the sharing.

So, I'd like to understand a little bit more on the engineering side. I'm not an expert by any means but I would like to understand what people think about the scale and the cost of this implementation if we get on the path of buying into a central certifying body or having the vendors test every application that our patients or researchers, or the market develop.

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

And this is Tim McKay with Kaiser Permanente, and a couple of things to add to the discussion. Any time any new software or access is introduced into the system there is significant cost and consideration in a couple of areas that I haven't heard talked about here very much and one is regression testing, so making sure that you have pounded that application to look at not only the happy path but all the things that could possibly go wrong because it's the exception path where typically the issues with privacy and security are going to be found.

In our experience when we're building software perhaps 20% of the system requirements deal with actually getting the thing that you're trying to do, while 80% are looking at what could possibly go wrong and how can we mitigate and understand the system behavior when things don't act as expected? So, that's why I said earlier an initial certification will get you so far but there is significant caring costs for any application that you allow to interact with an existing system.

A second area that I think we're seeing really good progress within the industry and expect good things to come from it, but one thing that hampers a system of being able to get information out of any kind of existing dataset is dealing with identity.

And when we're receiving a call to extract data through kp.org for our portal we're doing so in context of having a known identity. If we open up to personal APIs the identity becomes a little more complex. So, what is the relationship with establishing identity with the App with establishing identity with the system of record that you're trying to get data from?

And while we're seeing good things say from the initiatives through NIST and the Identity Ecosystem Steering Group in relation to forming a persistent identity that can be used for access to multiple secure services the system requirements and how this would work really in the field against medical datasets is still being worked out.

And so we do see that there is promise for being able to open up to a broader set of APIs and Apps that are using say APIs that we develop and provide for interacting with our systems but it is not trivial to integrate and working to make sure that we have the right person accessing data that they are

authorized to get and that the data is being extracted in a way that is protective of the patient's privacy are very, very important things for us to address.

Brian K. Lucas – Enterprise Systems Architect - Aetna

It's Brian Lucas from Aetna, Tim I'd pile right on top of what you said. I think one of the challenges that continues to face the healthcare system and I will speak beyond my current role in Aetna now as I have a role on both provider side and payer side.

There's a couple of problems with privacy and security of APIs and we've touched on some of them, right? There are problems with a verifiable application identity. Is the code that's trying to access my API the code that's supposed to be accessing my API?

There is a user account problem. Is the user who is sitting behind that code really the user we think they are?

And then there's what I'll call a linkage problem. Each data store, each company, each provider of information has got data organized around humans, if you will, call it in individual identity. So, for example, Facebook has a credential for Brian Lucas that's a user account identity. Aetna has a profile of Brian Lucas the insured, that's an individual identity and the final challenge is ensuring that the human on the other end of the system is really the human they say they are i.e., they match the credentials that they've presented to the application code that's granting them access.

And that this account, that electronic account, and credentials is properly linked to the correct back-end individual identity data and then further that while it's linked it is also authorized to access that back-end data and that's that three-legged problem of the human against the credential, the credential linked to the back-end data I think is where most organizations face significant challenges of trust and verification in meeting the ultimate goal, right, which is "is it really Brian Lucas looking at his personal data or someone Brian Lucas has authorized?"

Paul Matthews – Chief Technology Officer – Oregon Community Health Information Network

Or...

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

And Brian to add onto that sometimes even when we get to a system of interoperable strong identity where I can get an assertion that I truly believe that the person who says they are Maria Gonzales is Maria Gonzales. My question then is for the over 5000 people who live in Los Angeles County with the name of Maria Gonzales that I have records for which one do I bind to and do I have enough attribute information in order to correctly link the accounts before I make the disclosure?

Brian K. Lucas – Enterprise Systems Architect - Aetna

Yeah, I think that's spot on, right, you've got to get the right human connected to the right data in a way that is manageable, retractable and auditable.

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

So, let me...this is Aaron Miri, I'm one of the committee members here and I want to touch upon what Dr. Kelly I believe mentioned earlier with ePrescribe. So, there are already companies such as Dr. Kelly's

company that are doing ePrescribing for narcotic substances and doesn't that meet all the criteria you're speaking toward so there is already precedent?

Brian K. Lucas – Enterprise Systems Architect - Aetna

There is precedent, I agree, I'd say there are dozens of them and that's the problem, right? The problem when verifying a human is one that's faced by every IT system that grants access, right?

And sitting sort of on the, you have to deal with the whole world perspective, right? New technologies, new companies, new methods, new standards are constantly evolving. Should we pick that company over this company? Is OpenID secure enough for our method? Is it widely adopted enough to hit small provider and remote member access for example?

Yeah, I think there's plenty of precedent I actually think that's one of the industry challenges is there's so much precedent it's hard to get down to...

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

Right, so, I mean, without trying to solve the problem I think we're trying to find a business case more with these discussions and I think the business case is, is API facilitation the right vehicle or mechanism to facilitate information transfer? Now to what level, to what specific widget, whatever, you know, technical jargon we can probably sit here and argue all day long the pros and cons, but I think, generally speaking, are we all in agreement that API facilitation is the right method once you get past all the other hurdles?

Brian K. Lucas – Enterprise Systems Architect - Aetna

Yes, it's Brian again, I would agree with that. It's the most recently presented technology that allows controls particularly with protocols such as Open Authorization Framework 2.0 on both the supplier and the consumer so that there's a dual set of controls. I think that APIs are the way that's going to happen.

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

Right.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

This is Leslie and I'd like to comment on this. It seems that we have precedent for processes that allow for people to identify themselves to the organization. I think when I go to Wells Fargo and open up an account I can't open up an account without my ID. When I receive my account I get a user ID for my online services I can then set my own password. I can then attach into it or Mint.com, a data aggregation service, and then have that participate with perhaps an App of my choice connected to the data aggregation service API. So, that's one method.

But, I do think that in healthcare we already have the precedent when a patient presents that they identify who they are, they provide a picture ID, insurance cards if they have it, and then they're granted access to the patient portal which I would I imagine in the same way would be granted access to the patient portal and granted access to the organization API so that they can attach the App of their choice to that but we've known who they are and assigned those credentials.

Then, as the patient uses that functionality they may then pull that data into the App of their choice or a data aggregation App, or another service so they can have everything all in one place. But we can't do

any of that without some identity proofing at the provider level and the API technology. So, that's a comment.

And then a question, there is risk, obviously, associated when you get data but there's also risk when data goes in and I wondered if the group would comment, I see a patient gathering their information from their App or the API to their App of their choice but they also have information that's going to go back into the record as patient generated health data.

Do you see that there's any sort of hierarchy of security or constraints that you would see different from a requesting data API versus an inputting data API from a new stakeholder like the patient or maybe the payer, or maybe the caregiver, or others in the care team?

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

Yes, so, this is Tim and would like to comment on that. That's pretty much where we're taking Interchange at this point in time is that instead of so much focusing on the data out in terms of personal health data we're looking at the data in issues.

So, what the Interchange platform allows for is an intermediate place that is certainly a protected dataset but is not a part of the EHR in a formal way where data can be aggregated and then based on the use case data can then be pulled into the EHR, you know, with certain permissions and controls.

But the initial approach that we've been taking has been looking at specific types of devices and ensuring that we can get the data in, in a way that not only gives us the raw data but enough metadata that it becomes easier to decide how to use it for clinical decision-making.

So, for example if we have any random glucometer that is pumping data into the system do we even know the thing was FDA approved? Is there enough metadata and provenance that the clinician can trust that those readings are accurate from a calibrated instrument?

So, for some consumer grade devices it's not quite so important. If your step count is off and you've got an error rate of 5% it's not quite as critical if you have an error rate of 5% and you're looking at glucometer readings.

So, the short of it is that we're, initially at least, looking at how we work with specific consumer devices and in particular how do we attach the App or the device to the dataset becomes a critical question in that this methodology needs to be smooth and clear so that we're getting the right data from the right person pointed to the right part of the data.

And then from there looking at issues of then how do we normalize the data in a way that makes it possible to use aggregated data from different data streams and inform something meaningful that can be used by the patient and by the clinician for improving their health. And so...

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

So, this is Aaron Miri, I want to...that's a good point you just made there. Let me ask though, I believe Dr. Kelly since you are both an ED physician and your company does work with an API gateway related ePrescribing, can you explain to the committee both sides of the coin, one, how can you trust the data that coming to you for either home medication reconciliation or prescription of narcotics for the data

that came into you as a physician and then on the flip side, have you guys learned any trials and tribulations about that validation, again, that sort of that data quality aspect and the importance of that?

Sean Kelly, MD, FACEP – Chief Medical Officer – Imprivata

Yeah, absolutely, thanks, Aaron, I think, you know, what we've learned from the ePCS process is that, you know, the process isn't easy to supervise enroll and identity...credential and identity proof people. When you have a captured audience like providers that need to perform a certain function you can ratchet up the security levels and, you know, obviously when someone is transacting and affecting the...and putting data into the system that system needs to be linked to really making sure that you identity proof in a way that is sort of the highest level security.

And so that gets to the question of, you know, do you treat data coming into the system different than the permissions and the authentication level and security level needed for someone just to access and view the system, al la, Mint.com or in our provider system, you know, we have a magic button where can view another EMR that we're affiliated with that I, as a provider, can view but not actually change the medication list when I do the medication reconciliation but I can make a note in my own record that will then sync up later.

So, I think that like many things we're talking about there are different levels of permissions and different levels of authentication, voracity, if you will, and I think that one of the things that should be inserted into the discussion is a discussion around biometrics. That is certainly a part of the discussion when talking about ePCS. And often times a biometric is in there to address that concern earlier when you talked about, you know, 200 Maria Gomez's in one area and sorting through to make sure you really have that level of comfort that the user piece of that level of security is actually correctly identity proofed, authenticated and then even you can add permissions in when you have patients allowing permissions and providers to be able to view their records as well.

So, I think that, you know, in conclusion, one of the major things we learned is that there are...yeah, there's a lot of companies out there that do stuff, there are a lot of innovative ways to ID proof, credential and grant permissions to view and to transact data.

I think it's up to standards committees to say that, okay for access to data where you're just viewing something and you're a patient then you need to meet these three criteria and when it comes to a provider level the level may be higher and you actually need a biometric attached if you're going to go in and actually transact and change something.

So, I think that, you know, that's sort of what we're coming to both on the provider level and the vendor level is that there are obviously different levels of permission and depending on what that user is trying to do then it's ratcheted up and somewhere in the mix often times is a biometric or at least some kind of one-time pin token.

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

That totally makes sense. And as a physician then I guess that gives you the level of reassurance once you receive that data, see that data you're able to make a clinical decision based upon that data because it is authenticated and it's valid.

Sean Kelly, MD, FACEP – Chief Medical Officer – Imprivata

Yes and I think that, you know, once you dig into it the devil is in the details. So, you know, I mentioned earlier about code status and healthcare proxies, and living wills, you know, orders of life-sustaining treatment that's one of the key pieces of information that we look to get and there are...there are...our kind of initiatives going on in all the...many different provider systems, including my own and several I'm sure on the phone, where we're trying to get that data accurate within the EMR but it's not enough to have it just within the EMR, because as you know, that can be hard for other places to access and particularly as an ER doctor I see this happen where someone can be coming from across town from another nursing home because they're closer to me they end up in my ER. I can't get at their end-of-life wishes and can't get at that documentation to understand what those are. So, being able to have that data available, this is high-level data that needs to be accessible, you know, and being able to have that and understand.

And certainly if I'm going to go in and change that code status then that needs to be the highest level of authentication possible and a comfort level on my part if it's going to change treatment and many of these pieces of data, as you guys have said, do change and potentially change treatment. So, there has to be a high comfort level on all those issues of security that were mentioned both the level of the code, the user, the linkage problem that was mentioned.

You know the area I deal most in is the user level, authentication and permissions, and ID proofing, but just to reiterate, you know, once dig into the cases it's not just about allowing the patient access but it may be that this patient delegates access to their healthcare proxy or in the case of minors it may be that you actually need the parent to login and, you know, which parent is it legally, you know, that's allowed to do that.

So, there are certainly a lot of security concerns in that aspect that need to be worked through but I think that, at the very least, acknowledging that there are different levels of permissions, different levels of authentication required. You can't require every single user to have a biometric just to view their data in their My Portal as a patient but certainly for providers at least I think there should be a higher level of authentication including one of those things either an OTP token or some sort of biometric in order to make changes in systems that may affect the other systems through the API connection.

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

Wonderful, thank you.

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

Okay, Meg Marshall has a question.

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

Hi, yeah, well, thanks to everyone what a great conversation. I have a question and Dr. Kelly you may have just touched on it a little bit when you were referring to permissions but it's in regard to some level of scope negotiation so that access is actually less than the full dataset that's available.

So, maybe a more granular level of access there and in particular I'm thinking of a couple of use cases and they may not be right on but nonetheless so, 42 CFR Part 2 data for example and restricted data or data that a patient has indicated to his EHR provider exercising his right to restrict access to a payer.

So, recognizing that if this is a consumer-facing App that the access should be consumer directed and navigated.

Do you have any experience with more granular levels of permissions and if so if you could of course explain a little bit to us about that, but also interested in hearing what types of education or what types of interaction you have for the consumer so that they are aware that they are exercising their rights in a particular way?

Sean Kelly, MD, FACEP – Chief Medical Officer – Imprivata

So, this is Sean. We don't have direct experience with that from the sense of direct to consumer or direct patient Apps or applications. On the provider level most definitely we have differing levels of the allowable authentication methodology and the levels of ID proofing.

In the case of just logging into an EMR we allow for batch tap through proximity, password, many other methods where we trust the hospital to credential that provider and monitor that and sync to the active directory. Whereas with ePCS it's a much more strict and auditable procedure were only certain FIPS compliant devices are allowed, etcetera, etcetera, that pattern on the provider side is, you know...we don't need to reinvent that wheel. I think that there are ways, particularly within the provider, the core of provider users there are ways to sort that through. I think it does become more complicated when you reach out to patients directly as has already been discussed and you need to make those patient or consumer facing Apps very clear.

You know I'm somewhat familiar with the idea of trying to restrict access to certain parts of the chart or not that I will tell you, just as a doctor, that becomes difficult because while someone may try to...some consumer or patient may try to restrict access to example, HIV status or psychiatric conditions, yet the medication reconciliation is not covered within that. I can tell you most of the time whether a patient has HIV or depression by their medication list and, you know, that sort of a rather obvious example but it shows you that some of the discrete data points it's harder to separate that out when you're dealing with actual patient care.

You know another example is a PDF of a discharge summary where someone may mention that, it's not searchable data, it's hard to sort out that HIV is mentioned in there or not without going deeper into that. So, as far as the privacy issues there, you know, that again gets messy in the real life of healthcare.

So, I think, in short, we have a fair bit of experience and comfort with the provider Apps and the provider connections in and out of that, less experience with the consumer-facing and I'd look to others with answers there.

Brian K. Lucas – Enterprise Systems Architect - Aetna

It's Brian Lucas I can speak a little bit to that. I think it also helps to go back to the distinction again between the consumer and the application. In the case of applications that have no users, direct users, then what you're granting access to is for that application to be able to get at data through your API layer, right, so that granularity of control I think is best implemented in controlling which APIs a particular App can get. So, that's the first throttle, right, and that goes back to all those proved conversations about is the App behaving correctly, is it vetted, what can the App get to.

I think there's a second conversation on top of that which is now what can the user of the App get to and that brings you into the conversation about scope grants, which is where the question is put I think.

An App may ask for access to say personally identifiable information but not protected health information and the user, in the protocols such as Open Authorization Framework, gets to decide whether that particular App is going to be allowed to access the data they own. That works on the consumer side. It doesn't work so much on the provider's side, right?

On the provider's side when you're accessing someone else's owned health data that starts to become a delegation model problem. For example, do I have a Power-of-Attorney to go after this individual? Does my role, as a provider, grant me access as a protected entity under HIPAA which grants me the ability to look at your data? What user control can be put in place?

For example, in divorce situations a privacy request may be placed between divorcing spouses were normally they'd be able to see data they can no longer see it and in fact a provider might want to be blocked by a particular spouse for fear that this information might make it to their estranged partner.

So, I think you kind of have to tear it apart into what's the App allowed to get to? What's the user allowed to get to? Do they own the data they're getting to and is there a delegation model in place?

And I think any industry help in defining and normalizing that would go far to helping App developers do the right thing without having to chase every individual developer.

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

Well, thank you for that, this is Meg, and if I could I have...maybe overlapping in a couple of concepts and for that I apologize, but this question is directed at Stan.

We've heard you...and this is something I believe that is an interest of yours, semantic interoperability and when I think about Brian's answer and defining a delegation model and normalizing that data I immediately go to semantic interoperability, you know, agreeing on the details of the data elements itself not just the API.

In your experience and in your plans as you're going through and thinking about how to implement your consumer-facing model what are your thoughts on the current environment that supports that? Do you see that potentially being a barrier for us as we move forward with our concerns around privacy and security?

Stanley M. Huff, MD, FACMI – Chief Medical Informatics Officer – Intermountain Healthcare

Well, I think, you know, my short answer would be that there's work going on and we're making progress but there's a lot of profile making and standardization of, you know, the data and the terminology to get to true somatic interoperability and, you know, I've been learning, through this discussion, you know, because I have focused much more on the clinical data and that semantic interoperability part then on the security issues.

So, you know, I appreciated Josh's comment before, but, I mean, my comment would sort of be the same one that I made before. You know if I'm going to create a community where my application can attach, I don't want, you know, one set of people using a certain configuration of OAuth 2 and a different organization using a different one so every time that I have to attach there's a whole...not only a different conceptual framework but actually a different technical way that I manage that.

I don't want to have to know, you know, how I attach to Kaiser Permanente and know a different way that I have to attach to the University of Utah, and a different way that I attach and authorize to the VA. I want that to be absolutely the same everywhere.

And, you know, coming back to some of the questions that were posed I can see where, you know, conformance testing could get in the way of that if it's not done efficiently. And I also see, you know, the potential, you know, when you start thinking about the combinatorial, you know, I've certified that my App conforms to a certain configuration of OAuth 2 but I don't know whether that App is going to be safe when I attach to a particular system and so...but it really should be at that level.

So, I mean, you shouldn't have to certify every App for every provider for every platform. It should just be, you know, one certification of the App against a given platform and that's still a lot but I guess I don't see any other way around it. So, given that, you know, I think we just...we've got to make the process of certifying a very automated process and a tooled and supportive process to do it. So, I don't think I answered the question you asked but...

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

Hey, Stan, this is Aaron Miri, so, I appreciate your comments and I can appreciate the technical especially having an engineering background but I mean, I continue to say to this committee and to all the panelists, you know, what I see as a CIO is, you know, the finance, the banking industry, all these other industries that do this already, I mean, heck, I applied for a car loan on my Chase App got approved took it to the dealership and bought a car without ever stepping foot in a bank. They authenticated me and knew who it was and approved me.

You know if my daughter presents to an ED and say Dr. Kelly is her doctor and he needs to know that she's allergic to penicillin. I mean, that's just the reality of it. So, I think if we give guidelines and specifications it's out there, I agree with you we don't want too much variability but we've got to do something because right now, I mean, it's a major deficit.

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

Dr. Miri, this is Aaron, I really appreciate you bringing that up because that was kind of the way I was trying to formulate a question about the trade-offs between, you know, trying to, you know, set a very high bar with regards to patient safety and helping data flow especially, you know, I follow the train of thought with regards to clinicians providing data to other clinicians.

I wonder if there is a difference, and this is a question with regard to patient generated health data, obviously a clinician would use that information to make some clinical decision perhaps. Do we have to hold say patient self-reported information to the same level of standards that we would to other clinicians?

For example, just so that I'm clear, I've got a hypertension drug that I'm taking and I choose not to take it when I need to be really alert because it makes me tired. So, I'm not taking it right now my doctor doesn't know that, but I could report that to her through the portal. Should my level of authentication be the same level as a clinician reporting that or is there a difference because I have a relationship with that doc and the tools we're using may be different?

Sean Kelly, MD, FACEP – Chief Medical Officer – Imprivata

This is Sean, I'm going to answer that as an ED doctor. All information is valuable if you know the source of the information and so your example is a perfect example, you have more accurate information about whether you're taking your medicine right now or not.

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

Right.

Sean Kelly, MD, FACEP – Chief Medical Officer – Imprivata

If I were allowed to see that information and also understand where it came from that would help me sort that information and understand the value of it. This happens numerous times that we go in the room and say, you know "do you have heart disease?" "No, I don't have heart disease."

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

Right.

Sean Kelly, MD, FACEP – Chief Medical Officer – Imprivata

"Well, what's that big scar on your chest?" "Well, I had a bypass and now I don't have heart disease anymore." Right.

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

Exactly, exactly.

Sean Kelly, MD, FACEP – Chief Medical Officer – Imprivata

That literally happens every shift where, you know, someone...and yet someone may have more accurate information about their, you know, blood sugar. And a lot of patients actually know more about their bodies and about their medical conditions than we do. They actually catch inaccuracies in the records more than we do.

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

Right.

Sean Kelly, MD, FACEP – Chief Medical Officer – Imprivata

We've seen this with OpenNotes that's another whole discussion, but, so what I would say is that I fully welcome any inputs into the system as long as it's clear the permissions that were needed to get that information and the veracity of the data is verifiable through a...you know, that kind of...you were talking about a more granular system of understanding kind of the permissions and where that comes from. So...

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

You seem to...using the API technology is there a way to track the data provenance for patient generated health data that's...that we should be jumping on or is it still pretty...it requires significant engineering and research to figure out the answer?

If you are approving the Apps that have access to your applications and I'm going to Brian's comments, and you know this application originates from a consumer, do we need more granularity than that as far as just the PGHD data provenance context?

Brian K. Lucas – Enterprise Systems Architect - Aetna

So, it's Brian again, I'll come in on that if that's okay?

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

Yeah, please.

Brian K. Lucas – Enterprise Systems Architect - Aetna

Yeah, I think this is tied up with the conversation on semantic ontology and the level of access. I think it's all tied together, right?

Data provenance is an important piece of metadata. The problem I think that users face is that the data in our healthcare system today is replicated, duplicated, re-combined and re-factored in systems in many, many places and for them to get any rational understanding of the data provenance and draw a conclusion about it might be challenging. I think it's necessary, but even if you look at something as "simple" as having an outpatient visit, simple he says in quotes. The data collected regarding that visit passes through a myriad of systems.

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

Right.

Brian K. Lucas – Enterprise Systems Architect - Aetna

And you have to ask yourself the question, which of those do you trust the most? Because you're going to trust all of them because they're all part of the protected HIPAA network, right? But did some system remap the data values for a condition code differently using ICD-9 and ICD-10 then the other system did and did we lose some semantic understanding during those transformations? And I think that's a very challenging problem that goes along with semantic ontology issues about the provenance of the data feeding that ontology to the API layers.

Stanley M. Huff, MD, FACMI – Chief Medical Informatics Officer – Intermountain Healthcare

This is Stan Huff, I'd like to make a couple of comments.

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

Please?

Stanley M. Huff, MD, FACMI – Chief Medical Informatics Officer – Intermountain Healthcare

One is, you know, I really...I think I like the paradigm a lot better of basically having good enough security and tracking provenance with the data so that the users of the data can make rational choices about whether they trust the data or not and it seems to me that it would get complex and very difficult to manage if we had one level of security protocol if I'm going to write data, different if I'm only reading it, different yet again if I'm a provider, if I'm a...you know, I think we're a lot better off to say, look you...it doesn't matter who you are the data could be important and the data could either save you or cause you injury if it is improperly used. But that's...so I would argue let's have, you know, a level of security and a process for security that is actually one process and we trust it for all of the things that we're doing, but we keep provenance on the data so that we know, you know, who...what system it came from, what person put it in, what kind of device it came from because all of those could be very important for the interpretation and use of the data. But I think that's a better way and a safer way than trying to make a very...a series of very complex different security protocols based on who I am and what my role is and other things. So, that's just my opinion.

The second thing is an issue that comes up, you know, from time to time and is very important and that is, yeah, right now, you know, I can get CDA documents from the University of Utah and I could ask for the data today and tomorrow when I get that data there could be...I get CDA document today and then the next one tomorrow and, you know, 98% of the data is going to be the same but 2% is not the same and so yeah, you get these echoes of data around the system. I can then, you know, make a CDA that I export to somebody else that might include some of the data that came and so, I mean, one thing...it doesn't all those problems in any sense, but sort of a founding principle that we should have is that if you're the original source of the data, if you're the one who originally collected it and observed it you have the responsibility to assigning a unique, globally unique instance ID to that data so that wherever it...and that needs to go with the data everywhere it goes so that if I get the same data from two different sources I can actually recognize it if it came from the original source.

And that seems to be a principle that we need to state somewhere and make a part of the architecture because I don't think you can...you can't have rational data maintenance otherwise, we've tried it. There is no combination of rules to recognize...you know, we did things simply, well if it's the same test at the same time on this patient we know it's the same that always fails because we didn't think about, you know, two simultaneous measurements on a renal artery, you know, left kidney/right kidney thing.

I mean, you just...so it seems to me that we have to have that principal that we start propagating as a policy in these systems that if you're originating source data you have to create a global unique identifier for that instance and that we all then respect that and carry that unique identifier with the data so that if I get that data again from a different source I can recognize it and I can recognize that redundancy and deal with it.

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

And that's extremely helpful. I'd love to hear from Tim as well about, you know, specifically is there a common minimum bar for providers and patients with regard to how they interact with their healthcare data or in your experience from the work that we've done on the HIMSS ID Management Task Force do you think that there is...you know we should all be doing what you do for providers at KP for example?

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

So, let me talk to aspects of that and then if there is something more you'd like to know about please let me know. I think there is always a problem with trying to design systems to big ideas. It takes moving things down another level of abstraction and looking at specific use cases and then aggregating the use cases and seeing what are the commonalities and can we abstract a more general way to deal with the data issues or not.

But with patient generated data part of the problem is most consumer grade devices are meant to collect data for monitoring personal health as an individual. They really aren't set up for being able to do information sharing with others and as such you have to kind of think about, well when is consumer data really helpful to a person's care? More broadly in relation to working with the clinician versus when does it become noise?

So, if I let in every bit of data that is being generated from a Fitbit every single day on a million of our users we have a massive data problem without really understanding what is the use case and the need for it.

So, on the other hand, if we get down to more prescribed use cases that we're trying to answer this particular question it becomes more apparent than what the data needs are. So, that frankly is the process that we're going through now at Kaiser Permanente is trying to understand when is consumer generated data very helpful for self-management of care and when is it helpful in shared management scenarios and, you know, what do we need to be attached to the data?

You know I would think at a very high level you need a date timestamp, you need some information about the device and the device manufacturer. You need some information about what entity is the data bound to. So, especially if you have more...a device...some personal devices are very personal, some are shared by more than one person and then how do you differentiate the data stream that is coming from that device and attaching it to the appropriate dataset.

So, a long way of saying is it becomes easier to look at the system issues when you get to the use case level. Looking at multiple use cases you dig into abstract what the minimum dataset needs are and then you begin to understand, for certain use cases, where you need an augmented dataset and that becomes a required part of any data coming into the system.

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

Very helpful. Thank you, sir. It's just a real thrill to be able to work with you guys and hear your inputs. So, you talked a lot about devices and in some cases like...in the scenario that I gave earlier I'm the device reporting that I'm not taking this drug it makes me tired. I can see your...I totally see your point about the difference of that use case versus, you know, I've done 400 steps today and been all sedentary all day and I totally hear what you're saying. And the trust and the authentication of who that source is may vary as well if I'm understanding you correctly.

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

Well, and I think you raise another point with that as well. Sometimes data from the devices is not sufficient in and of itself but you actually need the patient narrative associated with that data in order to understand it and interpret it.

So would your doctor for example, as the one-time instance, want to make a change to your medication or has this been something that you've been reporting they can look at the device data and then make an informed clinical decision, you know, based on aggregating those...clinical judgment.

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

Thank you so much. Michelle, you should probably take it over I can talk all day with these guys.

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

Josh Mandel?

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

Thanks, Michelle. So, I have...maybe I'll just ask a very broad question among the panelists, you know, representing the sort of healthcare delivery perspective, do you think that patients should be able to bring whatever Apps they want to the table vetting or no and it should be up to providers to set up the proper rate limiting so that, you know, no matter what malicious thing an App tries to do it would just

be prevented from doing it by the infrastructure itself just the way that, you know, I can register an App that asks for access to my Google Docs and if my App starts doing something malicious Google will automatically shut it down if it detects too many requests per second. Is there a general sense that patients should be able to make those choices or do they need more protection in place from provider organizations?

Sean Kelly, MD, FACEP – Chief Medical Officer – Imprivata

I'm going to answer this one just because I'm a Hospital CIO right now. So, today I allow patients to bring in on CD, via cloud, secure cloud whatever the else PACs images be it cardiology or radiology images, it basically goes into a broker where let's say it's radiology so a radiologist or a radiology tech would look at the pictures and make sure that it's DICOM quality clinically viable and then they would import that into PACs so that the radiologist or whomever can make a diagnostic interpretation. So, we do that today.

We allow for images from wherever, I don't care what modality, I don't care if it came from a Phillips system or a Siemen's system or whatnot outside my organization because I want that data, I want them to bring in those priors with them.

So, if we do it today and it's generally acceptable principle most hospitals do that why can't they do that with data on applications? What's the difference?

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

So, let me just respond very quickly to that because it's an interesting parallel in some ways, but I think the key difference between the scenario you just described and the one that I was asking about is in the scenario you described there are humans in the loop who are checking and verifying things on a one-off basis and so data aren't just sort of flowing they're introduced by a broker.

But the other main difference I think is that the scenario that you brought up is one about a patient putting data into your healthcare system and the one that I was specifically focused on or the one that I tried to asked about in my question was about patients who want to connect Apps that will access their records that will read all of their structured healthcare data out of their EHR.

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

This is Tim, I would be very slow at this stage of the state of the art is not quite there yet I think to offer that complete broad access. I think a path to getting closer to that is to have model systems that are set up with specific Apps that provide the functionality that the patient is wanting and needing to extract their data but to look at not only the connection and pulling it out but then what is the full workflow for this persisting and then can we provide some sort of minimal vetting.

I'm just really hesitant to say bring anything you want when I know how bad App security is. I know how bad terms of uses can be structured so that people are...essentially there is no transparency with what's happening to their health data and I don't want to be complicit in that type of data access.

So, it's something where certainly, at Kaiser Permanente, we see the benefit of having aggregated data because we are a system where we are provider and payer and many, many of our patients have years of their medical records or say their only medical records are at Kaiser and being able to get that high combined view is extremely helpful.

So, we sympathize with the problem but I would just not open up our system so readily without understanding what the pitfalls are in order to even be able to give good informed consent to the person who is attaching to the system that we have a reasonable expectation that their data is going to be used in the ways that they themselves intend it to be used.

Stanley M. Huff, MD, FACMI – Chief Medical Informatics Officer – Intermountain Healthcare

This is Stan, I want to agree and disagree. I agree that Intermountain would not be able to do it today. We would not be able to open it up, you know, we don't have the protections in place and so we need to step into that carefully that's the part I agree with.

But in the long-term that's our responsibility and that's what we need to do. We need to put those protections in place so that we can...yeah, if there's a rogue App and it's asking, you know, it's throwing out, you know, 20 queries a second and it has the potential to bog our system we need to put those protections in place that's our responsibility because I don't see any other way that it would work.

And we don't have them in place now but I think that's our responsibility and what we need to be planning and architecting for is that we can protect ourselves from rogue applications. Because I think anything else is going to...is not going to have the impact that we want to have on the choice in software and the flexibility, and the...to get the real market advantage of having thousands of developers out there.

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

Given your guy's experience over the last...

Stanley M. Huff, MD, FACMI – Chief Medical Informatics Officer – Intermountain Healthcare

And...

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

Five or six years with Meaningful Use and so forth do you see that as a function of a legislative process, a government process, a regulation process or a market process, or association process whatnot?

Stanley M. Huff, MD, FACMI – Chief Medical Informatics Officer – Intermountain Healthcare

You know I see it...yeah, I would...I think it would be...I would see it ultimately being something that's market-driven and that is driven by our desire to provide the highest level of service to our customers but I think national discussion on it so that we're agreeing and we can develop best practices together is very helpful but I would...that's the sort of thing that I'm really nervous about coming as either a legislative or regulatory mandate.

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

Yeah, is there an all of the above option on that one?

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

Well, I actually had just read the...the latest draft of 21st Century Cures that's why I was asking.

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

Right, right and this is Aaron Miri. So, I think I would also answer that I think it's a little bit of all. I do think there needs to be a WIIFM, a what's in it for me, aspect somewhere in this discussion. I think it's beyond the technical construct of an API discussion because there is a national outcry for data

facilitation and sharing and there's a lot of other barriers, non-technical barriers, that hold organizations back and/or competitive advantages.

So, I think it is all and it's going to take both a carrot and a stick to make this happen because even given those discussions and those types of legislative movements there's going to be a lot of reluctance because data is power. I mean, there's a monetization of data going on and organizations are hoarding data because it's leverage for them. And so it's going to take a lot more than just technical constructs and legislation to get the ball rolling fully.

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

You know the...this is Tim and one bit of caution that I would interject and again, Stan wasn't...I don't think we're really in disagreement that the movement will be towards open APIs it's just the path of how you get there and the path of being able to do so in a way that honors patient's safety and patient security and privacy. Boy, I'm sorry, I lost my train of thought...

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

This is Michelle we're getting close to the end of the time for this panel and there still are a few more questions.

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

Sure.

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

So, Drew?

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

Yeah, thanks, Michelle. This is Drew Schiller, so I've just been sort of going through my head and thank you panelists for your comments this has been quite an insightful discussion. As I'm thinking through a lot of the use cases that have been discussed, you know, we've had an instance of, you know, can I...I can use my online bank to apply for a loan and buy a car without ever having to step foot in a bank. We've been...we had an instance of a description of, you know, an elderly person having an episode and delivered to, you know, one emergency room and not the other and that physician not being able to access that patient's data.

I'm just wondering, how do you panelists see the data being driven? Is this going to be largely a consumer driven initiative where individuals/consumers, so in the case of that elderly patient who is maybe unresponsive in an emergency room, how would that patients say "I want you to be able to access my data from the other provider on the other side of town" right? How would APIs in that instance help?

Because really, like...from...I think from what we're talking about as a Task Force by and large is more of a consumer-driven situation, you know, sort of a bring your own device solution for healthcare where the consumer is saying, I want to be able to access my data and put it where I want, right, I want to be able to power the Apps that I want.

I just...I guess I'm just sort of trying to think through my head, are the APIs going to be able to solve all the challenges or are we trying to primarily focus on consumer-driven? I'd really like to get your thoughts on that.

Paul Matthews – Chief Technology Officer – Oregon Community Health Information Network

So, I think, this is Paul, I think the simple answer here is that there is a separation of the two requirements. The provider-driven requirement is separate than consumer-driven requirements and I think that trying to answer these in one API or in one specific compliance security requirement is problematic, I'll put it as politely as I can put it.

The...I think looking at...if we look at the way that the consumers are accessing the system I'm in full agreement that any application should be able to be brought to the table and that we should deliver limitations of how many calls the type of data is being driven back.

The provider's side of the house I think today the limitations still come down to is the compliance side and this is not a major technical hurdle, it's an issue around compliance.

And every time I hear the conversation, and I hear this a lot today, it all comes down to, if we removed the compliance requirement, the technical requirement may become clearer, now we layer the compliance requirement back on top and we remove a lot of the technical discussion. I become very frustrated in the conversation and I apologized if it sounds that way. But I still see compliance as the blocker to all of this. These aren't major hurdles technically.

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

One of the...this is Aaron and just from the perspective of that particular obstacle or barrier from a compliance perspective I think getting consumers engaged so that before grandma showed up unconscious at the hospital she actually shared her privacy preferences and that we actually had a methodology of...such as we heard yesterday from the folks at UMA and otherwise, to better enable consumers to say "hey, I want that data to flow" before it's ever an emergent issue would be one way to also make this whole policy discussion, this whole compliance discussion simplified. But it may be very distant from now, you know, time may have to lapse before we get to that point.

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

And this is Tim, kind of picking up on what I was talking about before is the unintended consequences of rushing legislation. I think we saw this with interoperability where there were ways where we were on a path towards interoperability, we're starting to get there technically, we're starting to work on semantics but we have no...really no good solution to the idea of workflow interoperability. How does information get delivered to the right place so that it is understandable and actionable at a point in time?

In a similar way within the consumer space I hear too many use cases and one is that you're trying to extract information in order for Apps to be used at the consumer's choice. And then also using the APIs as a way to aggregate medical information sort of as a stopgap or a realization that we aren't there with medical records interoperability so that no one necessarily has your full medical record.

And I think it's still a space to explore for the community to start to delineate the use cases and then to start to look at model system design against those use cases with how can we meet the consumer needs? Because ultimately it's important for us to do.

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

Leslie Kelly Hall?

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Thank you and, you know, I think there is a natural tension between security and privacy and the difficulties that you guys have all brought up. But I go back to the Mint.com model where Wells Fargo doesn't know that I necessarily have the App MINT, I've given Mint those permissions. And I think that what...the natural progression will happen as patients have access to the Blue Button and they're able to download their record as they choose is that they will download this to Apps that are completely disassociated with the health system and the healthcare system.

So, to Stan's concern that you want to approve the Apps that the patients connect to and use, and I can understand that from a security point-of-view, but from the consumer point-of-view I should be able to use my data the way I want to and will it take education around that, absolutely it will. Will I have to learn what good Apps or bad Apps, absolutely.

But the days of being able to keep the data in a way that only is approved use I think is gone. And so patients will use the data in new ways, new economic structures will develop and technologies will develop to support that kind of consumerism.

So, the question is then, as responsible provider organizations around the country how do we set an infrastructure that allows the providers not to be completely disintermediated but to be included in this ecosystem as the patient begins to get more control of their data as they download data from multiple sources and aggregate it themselves and use it new ways?

So, this kind of shift is happening and I think there's an urgency for us to do the minimal requirements that I think was mentioned earlier by Tim, how do we start, you know, crawl, walk, run? We start small and have some way to integrate.

But I think the days of preventing things are over. And in fact the law requires today or the regulation requires today that the patient can choose the App they want to, to connect and so that is presented to us today and how we resolve that is important but it's to understand that the patient when choosing that App the burden of privacy becomes the patients. The burden of use is the patient's the provider is not...is no longer held accountable for that data usage and breach.

So, I'd like the group to comment on how we accelerate and speed up these kinds of access so that it is a combined ecosystem versus one that completely goes the other side where consumerism takes over everything.

Stanley M. Huff, MD, FACMI – Chief Medical Informatics Officer – Intermountain Healthcare

So, this is Stan, I hope I didn't say I anything that implied I was trying to corral the data in testing that's not the intent at all. My comments about testing of applications had nothing...I want exactly what you describe that the patient or for that matter providers, anybody can choose whatever App they want.

My interest in testing is so that for instance if I'm looking at this from the perspective of Intermountain Healthcare I can put an infrastructure in place that protects all of my users from an attack that brings my system down. That's the only kind of compliance testing I'm interested in it's not in any way trying to restrict the flow of data.

So, if I said anything that implied otherwise I, you know, want to correct that because the only kind of testing I'm talking about is testing that makes it safe and I can protect Intermountain's system from attack so that I don't have denial of service because someone has a rogue App. I think...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Yeah, I think that's completely reasonable. Thank you, Stan for...

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

Yeah, yeah.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

For making that clear. I think that is where...that there should be concern and a good credentialing system and a good infrastructure can help that but it is basically the patient's right to use their data any way they choose.

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

Yeah, and this is Tim with...

Stanley M. Huff, MD, FACMI – Chief Medical Informatics Officer – Intermountain Healthcare

I hope I...

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

Would completely agree with that. The concern is the layer for extraction and input of data. It's not so much that the consumer can't use their data in any way they choose too, certainly, that's a freedom and a given but it's the specific App that allows you to put data in and to extract data it's that layer that we care the most about.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Thank you.

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

And just a quick question. Do you feel that, you know, we've been supporting a number of different modes of exchange today not all of them currently exposed to consumers such as query/retrieve mode from the IEH gateways or, you know, using the Direct methodology. Is that good layer, an adequate layer, the best that we have for now until we get better at some of these APIs and introducing a layer for extraction and entry or is that not adequate?

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

It's developmental and I think it solves some of the problem and gets us father along the path, but I don't see that as a complete solution.

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

It's a starting point, let's not kill it, but it...

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

Yes.

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

We need to go father to support all the things we want...

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

Absolutely.

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

To be able to.

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

Absolutely, I mean, through kp.org today we completely support the Blue Button...

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

Right.

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

And if you have a Direct address we'll send it electronically through our portal as well. But we don't see again, that this is the end-state fit, it's sort of...

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

Right.

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

A stopgap for now.

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

It's a bridge useful tool at a particular point in time for some use cases.

Timothy McKay, PhD, CISSP – Senior Director of IT Product Management & Delivery – Kaiser Permanente

Yes, absolutely.

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

Thank you.

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

Okay, I think that's all of our questions and thank you, again, to all of our panelists on Panel 3. This has been a very good discussion and we greatly appreciate it. We are going to now transfer over to Panel 4 before we do that, though, we're going to take a quick five-minute break so we can transition over and make sure that we have all of our folks for the next panel on the line. So, for those who are on the phone, if you could please just step away and mute your phone if you need to do anything and we'll come back in five minutes and we'll regroup at 1:06.

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

My bladder thanks you, Michelle.

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

So, I know we're on break, but I do want to check and see if we have the panelists for Panel 4. I know there were a few people that wanted to make sure they were on the line so let me first just start, Ted were you able to join, I think I see that you're on? So, I know we're on break but I'll just check and see if any of the folks are here, so John Moehrke are you on?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

I am here. Can you hear me?

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

Hi, John, yes, thanks for joining.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Hi.

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

Chris Bradley, are you still here?

Christopher Bradley, MS – Chief Executive Officer – Mana Health

Yes, I'm still here.

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

Okay, thanks. James Lloyd? Okay so we don't have James or Ted. I think Ted is on though so maybe...let me make sure that one of our folks is on the line. I do see that he is on the web, but I think he needs to call into the number as well. So, John Moehrke is here. Ted, were you able to join? I was hoping that you just stepped away because it does look like you are on the phone.

Ted LeSueur, MS, CISSP, CHP, CSCS – Director, IT Regulatory & HIPAA Security Compliance - McKesson Corporation

I did just step away and I am online.

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

Great. Thank you, Ted. Chris Bradley is on and we are just looking for James Lloyd. He is the last person on the panel, so hopefully by the time we get to him, he will be on the phone. So, do we have Meg and Josh back?

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

We've got Josh.

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

Okay. Hopefully, Meg will be joining us soon and we'll get everyone back very quickly. I did hear a number of Task Force members who are back as well. So, let's go ahead and get started. We're already a little bit behind. So, John Moehrke if you're ready please take it away.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

I am. So, I want to thank the Task Force for inviting me to speak on behalf of GE Healthcare. I'm also the Co-Chair within HL7 Security Workgroup, a member of the FHIR Management Group, the lead of the IHE Mobile Health Documents and an active member of, and, advocate of the HEART efforts. So, I just wanted to make sure that background was understood. I am pleased with a lot of testimony you guys are receiving it is feature rich with fantastic comments and suggestions and that makes me even more pleased to have been invited.

GE Healthcare had been a strong supporter of standards-based interoperability. It enables us to be a global healthcare solutions provider. Any customization or specialization for a region or a particular provider organization is an effort that's counter to this and really is not helpful to us as a global vendor. I'm glad to hear that others in this testimony have given the same kind of solutions to use standards for their various reasons and I was actually excited to hear some of the reasons as well.

So, on APIs, GE has had APIs, you know, for literally decades. Most of these are the bread-and-butter of healthcare organizations, the network backbones drawing on HL7 and DICOM using IHE profiles to make them as reusable as possible.

Many of our IT products have web friendly APIs, some of them browser centric, some of them API centric and we have a limited availability of FHIR being used by a few pilot sites. This limited release is really more just simply due to the developing nature of FHIR and its variability.

All of these APIs, old and new, are guiding my testimony. RESTful APIs don't really fundamentally change privacy or security, although they do elevate the threat presented. We place no special qualifications upon our customers to gain access to APIs or documentation. Clearly, of course, APIs, you know, do have authentication and authorization restrictions so we rely on those means.

So, when it comes to the privacy concerns they mostly involve a shared role and responsibility between the healthcare provider and GE as a vendor. Given that GE doesn't have a direct relationship with the patient but the provider does and the provider has controls over the policies and use of our solution or either our software devices or services we in part...most of those privacy concerns are upon a healthcare provider organization.

Given this reality, we do have a privacy by design approach built into our product development process so that is there to guide our products to deliver the kinds of enabling technologies that the healthcare provider organization would need to support their privacy needs.

So the main problem that we see in privacy and security overall is really just a wide variation in security and privacy maturity of the healthcare provider organizations that we deal with. The very large organizations have a mature capability. They have policies. They have procedures. They have the technology solutions available and build this trust relationship and engage with us. But the vast majority of the healthcare provider organizations just don't have this full range of operational aspects. Add to that this variation and layering of legal and regulatory policies that we all have to live under just really adds a lot of churn.

So, some technologies can be used to solve these and, you know, we can go into those, but I don't know that this is as important to deal with the technology choices so much as the policy issues. Technologies are obviously things that have been talked about identity management both who is the patient, how sure are we that this is the patient, user identities, is this the provider, are we sure this is the provider.

Actually, when the patient is a user that adds yet another level of indirection which adds a level of unsureness to this. Authenticating those, managing of consent, managing of accountability, management of incidents really all of these are sparked with a variability and a need for policies and procedures. And we just really don't find those within the majority of healthcare organizations. Again, some we do so it's not to say it's not out there.

One of the things that I haven't heard discussed much is...and I'm kind of skipping over some of my written testimony because I really want to hit upon the really needs also as part of this shared relationship between the healthcare provider and the vendor is we need to come up with policies and procedures around incident detection and incident response.

Reality is that no matter how much technology we put in place something bad will happen and we need to detect it as soon as possible and we need to work together to remediate. So, I think that's something that I haven't heard discussed so I wanted to put a little emphasis on.

APIs imply a much more agile ability to hook different applications into services and this brings up policies and procedures and really technology questions around how do we identify trustable applications or even trustable services. No matter which side of the coin you're the other guy is always, you know, should I really trust them. And how does that...

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

Hi, John, could you please wrap up?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Yes. How does that trust translate into the maintenance across over time. So, you know, I think I've addressed that this is really a policy challenge and I'm really excited to put this in front of the team.

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

Thank you, John. Ted? Ted, if you're still ready, you can go ahead. Is your line muted, possibly? Okay, so we'll go back to Ted. Chris Bradley if you're ready we'll skip over to you.

Christopher Bradley, MS – Chief Executive Officer – Mana Health

Sure, yes. Thank you. I can go now. So, first and foremost, thank you very much to the Task Force for having me able to speak today about what we're doing and, you know, comment on some of the potential possibilities and challenges with APIs.

So, my name is Chris Bradley, I am CEO and Co-Founder of Mana Health. And effectively we are a vendor that allows healthcare organizations to leverage their clinical and patient-generated data through our monocloud data platform. And so what we do is we extract data from numerous clinical and non-clinical patient generated data sources and then allow access to this unified view of this patient...of these patients through our standards-based API. So, this really is, you know, something that we're very passionate about is enabling access.

We also have a background in patient experiences so we've developed and launched region-wide and statewide patient portals to give patients access to their data. So, we feel like this combination of the technologies underlying APIs and also patient involvement in both their healthcare and then in their healthcare data are key to pushing healthcare forward.

So, I think, you know, to sort of parrot what we've already said a lot on this panel so far I think the issues aren't so much the technologies of instituting an API. There are technological challenges but many of those have already been solved in other areas with high sensitivity to data privacy and security.

But I think some of the challenges that remain and that I think, you know, I'm really excited to speak more about are the security challenges around how do we enable rapid securing of the APIs and also the security infrastructure that we can all agree on and constantly evolve with new threats and then also the notion of privacy and ownership of the information. This is an area that's almost outside of the pure API sphere, but is critical to the question of once I have access to this data through an API how do I assign that ownership to the correct individual and access to the correct individuals and where does the hierarchy of that consent management...how does that hierarchy flow and who has access to what data at what time within that hierarchy knowing that a care team is involved not just a patient in using this data to enable better healthcare.

So, that's all I really wanted to say about us and then I'm submitting written comments for more of the questions and I'll leave it open to dialogue afterwards as well. So, thank you very much.

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

Thank you, Chris. And I think that we have Ted back. So, Ted, if you're ready.

Ted LeSueur, MS, CISSP, CHP, CSCS – Director, IT Regulatory & HIPAA Security Compliance - McKesson Corporation

I am and I apologize my phone cut out at the worst time. So, good afternoon and thank you for inviting McKesson to participate in this Task Force hearing. My name is Ted Le Sueur, I'm a Director with McKesson's Information Security and Risk Management Team. And today I'll be sharing our responses to

some of the questions that you asked of us from a vendor perspective. So, we'll be going through these questions line-by-line and I'll read the question and then I'll read you our response to that.

So, your first question was: Does our organization publish APIs for Apps that are available internally or to third-parties. If so, are they clinician-facing or consumer-facing or both?

So our response is McKesson has internal financial and clinical-facing APIs. Today, we have not published our consumer-facing APIs although that is planned for the near future.

The second question was do you publish your documentation online or make it available to third-party developers?

McKesson, while our approach might differ slightly from segment-to-segment in those that we serve, we provide access to third-parties generally through initially a request for an NDA and then we'll perform a technical review and apply mutual satisfaction of that review and that a relationship is technically feasible and of value. We would then require the third-party developer to acquire a software developer user license. Once that license is acquired then we would provide our API documentation.

Your next question was do they need to be certified by an organization to use the API?

So, while a formal certification is not required, adherence to specific user terms and policies are required and attested to by the third-party utilizing the API. As we consider broadening the reach of our APIs to consumer-facing applications, that are not currently bound by the same regulatory obligations as our current customer, we are considering a more formal certification process.

The next question you provided was, are there production deployments of these API/third-party applications using APIs?

Our response, McKesson does have deployments of our APIs in production today across multiple business units. For example, our picture archive communication systems or PACs and one content, which is our document management system just to name a few.

What are the perceived and/or actual privacy concerns or barriers to the adoption of APIs?

Our thought is consumer-facing applications are not currently bound by HIPAA and today there is not a generally adopted formal certification process or regulatory obligation. Patient consent is a critical part of the function and I don't believe that we have an adopted trust framework for consent management. We believe that a person should be in control of their health data and should be able to delegate in the authorized application to access their health record. Possible privacy barriers might include ID proofing and ensuring that the appropriate permissions are assigned and allocated.

Next question are what are the perceived and/or actual security risks or barriers to the adoption of APIs?

We would suggest the security risks are the same as any interaction between applications, ensuring appropriate access controls, authentication of the entity attempting to retrieve data or update data via the API are critical components. Assumptions that are made by both parties on this topic need to be clearly defined.

At this point there is not a common-agreed upon framework to ensure that the applications accessing the API are not bad actors. So there is concern that as the data securely leaves the API it may be incorporated into an insecure application placing an unsuspecting consumer at risk.

In the absence of a trust framework each vendor will likely define their own framework with varying levels of risk tolerance. This variance could result in less-risk tolerant vendors being perceived as information blockers.

And your last question was are their third-party certifying authorities and non-healthcare industries that we can leverage?

There may be a few but none that we believe have enough market share that would result in an overall Good Housekeeping Seal of Approval that the market would unilaterally adopt. Again, thank you for inviting McKesson to participate today and this concludes my testimony.

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

Thank you, Ted. James Lloyd?

James Lloyd – Co-Founder & Chief Technology Officer - Redox Engine

All right, can you guys hear me? Hello?

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

We can.

James Lloyd – Co-Founder & Chief Technology Officer - Redox Engine

Okay, good, yeah, thanks. So, this is James Lloyd, I'm the CTO at Redox Engine. We are...our whole team sort of has a background in EMR technology and interoperability in that space and for the past two years we've been working on a platform that allows certain modern-based applications to more easily integrate with health systems both on the provider-facing applications as well as patient-facing applications.

So, what we do is we create a standardized API for developers that can span multiple EHR vendors or even variances between different health systems and we provide that API access publicly so you can have a free developer account as well as use our developer tools to start building your application without needing to really engage directly with the health system as an application developer. And, you know, once you go on top of our platform then we sort of collectively go into a health system and work with that application vendor to make sure that they can meet all those security and legal requirements of that health system as well as go through an EHR necessary testing both the regression testing which we talked a little bit before here as well as workflow testing.

So, in the sense of providing any sort of certification or approval that really ultimately lies with the health system but we do help our application vendor customers review...we review all of their workflows and security setups and guide them through that process.

We are live in production today with a number of applications at a number of different health systems spanning a number of different specialties as well as multiple EHR vendors underlying them.

Yeah, and as far as general sort of concerns and things like I see this group working on, I think one of the biggest ones is the patient identity verification that we talked about, a few of the panelists had mentioned so far, so really knowing that the patient on the other end of that application is who they say they are.

One issue that I think is also coming up with patient-facing applications where they may not have a direct relationship with the health system is just how does that patient know, you know, if they need to connect to a specific health system to get to their data, you know, the way that the IP infrastructure for a given health system is identified may not be how the patient thinks about their health system. So, if I think about going to Barnes Jewish Hospital maybe that's part of the...system and really might need...that directory of IT systems to patient-facing consumer brands.

And the last thing I'd note here is that what we've seen is really the...the biggest bottleneck here is really one on the government side of things around making sure that BAAs are in place, security review and really I think a need for that sort of standard trust model and then agreed upon standard set of documentation and checklists for that sort of thing would really speed up the implementation of new applications. Thank you guys for your time.

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

Thank you, James and thank you to all of our panelists on Panel 4 and we'll now open it up to questions from the Task Force and it looks like Josh has a question.

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

Sure, so thanks to all the of the panelists and I thought I would start off with a question about what a few folks have referred to in this panel and also in the previous as a shared responsibility between healthcare provider organizations and vendors.

And I'm wondering if, in this panel from the vendor perspective, you can talk about what structures you have in place for exercising that kind of shared responsibility about determining the access controls, setting policies together and to what extent information flows from the EHR vendor out to the provider organizations like vendors tell providers "here's how the world works and here's your menu of options" or is there more bi-directional communication?

And to what extent are these conversations one-on-one between a vendor and one particular provider organization versus, you know, are there ways in which vendors work with a whole group of provider organizations? Maybe a lot of their customers all at once to work through these kinds of common issues?

Christopher Bradley, MS – Chief Executive Officer – Mana Health

This is Chris speaking from Mana. So, I mean, from our perspective I think there's two different elements to that question, there's the question of are there technical pieces in place to control access to information in the right circumstances and then are there policy and documentation elements that you can then use to both officially authorize that access and also document and track, and audit that access in the appropriate ways so we have both and we've put a lot of time and thinking into, from a technical perspective how you solve that question while at the same time trying to bring as much information to bear as possible to the people that are being authorized.

So, how do you aggregate information, how do you unify information around patients and still provide the level of access and control that's appropriate? And so we I think from a technical perspective that's something that's solvable and that we've solved but one of the things that we find still not a challenge but I think an open issue to scaling this broadly, the API approach broadly, is having very, very clear unambiguous and then hopefully automatable ways of determining how authority is given, who is allowed to give what authority and then that can lay the ground, the foundation rather for than automating that process with technology.

So, I think right now this sense that there are patients...patients own their data and that's something that is clearly understood that we have ownership over our own data. But how does that ownership extend into what circumstances when we want to give others our data for the purpose of caring for us.

So, I think that establishment of trust between the patient, the care team, the vendors involved and then the ultimate application you start having a lot of different people involved and I think just globally we need a way to unambiguously handle those use cases and then any exceptions they may have so that we can then set about creating a standard for those situations.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

So, this is John Moehrke from GE. Thanks, Josh, for the question. I actually would have to answer all of the above to begin with because...and it's much aligned with my message is that we just see a huge variability.

If we can work with a larger, you know, group of organizations that can, you know, be worked on a common set of roles and responsibilities of course that's preferable and one of the reasons why I'm actively involved in things like the Sequoia Project and even in Wisconsin with WISHIN.

But, often times it does boil down to a one-on-one discussion where everybody puts their, you know, needs or capabilities on the table and you go from there. So we would say these are our capabilities, this is two or three patterns that are being used elsewhere and it starts with a discussion like that. And unfortunately that's, you know, kind of the root of not a very reproducible solution.

But, of course, you know, one of the advantages of, you know, using APIs and doing things in an agile way is when you do identify a new need or a new capability you can much more easily adjust to that. That would be my answer.

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

Well, thanks to both of you. Anyone else on the vendor perspective in terms of how you work with customers to set up these kinds of shared responsibilities?

James Lloyd – Co-Founder & Chief Technology Officer - Redox Engine

Hi, this is James from Redox, I can talk a little bit about what we do. So, you know, by and large I think the current state of things, you know, I talk about the current state versus where we want this to go, but, you know, from our observation the current state is very much system-to-system so, you know, there is not...there is not sort of an application in use today or a thought that didn't have to go through a security review and a legal review from the health system which is using that application.

And I think, you know, some of the biggest challenges we have are going to be similar to the ones that I mentioned previously of we want the patients to be able to use these applications but we need to be

able to correctly identify both which system and which patient within that system is actually using that application.

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

All right, thanks very much.

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

Drew Schiller?

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

Yeah, thanks, Michelle and thank you to the panelists for your insight so far. So, I would of course really love to hear from John and Ted on this but I'd really like to address this question first to Chris and James. You guys, I've spoken to, you know, both of you guys before and I'm wondering from your boots on the ground perspective we've been talking a lot today about adopting, you know, like a common API framework for providers. But from your your perspective is this realistic or even possible as you guys are like working through these various systems for healthcare providers to actually adopt a common API framework in some sort of reasonable amount of time?

James Lloyd – Co-Founder & Chief Technology Officer - Redox Engine

Yeah, I can answer that.

Christopher Bradley, MS – Chief Executive Officer – Mana Health

Go ahead, James.

James Lloyd – Co-Founder & Chief Technology Officer - Redox Engine

Okay, cool. I think it's going to be a bit of a challenge given the current ecosystem. So, I think, you know, there's been a few references to comparing our healthcare industry to some others out there and I think one really interesting scenario that we have here is the balance of I would say optionality or extensibility within the current standards and maybe even some of the future standards that really make it challenging for a given application developer to know that there's going to be something consistent on the other side.

So, you know, today we have...even today we have EHR vendors who are, I would say, partially implementing FHIR to, you know, maybe 80% but then you might have Vendor A does one 80% and Vendor B does another 80% and as an application developer and now you have a gap somewhere in between that you have to fulfill and, you know, as an aside I think it's very similar to some of the early days of implementing CSS across different browsers and you have to kind of fill the gaps with your own sort of cleverness and I think that's really the barrier here is that the...you know a part of me wishes that these standards like FHIR were much less optional from the implementation side, that it was sort of, it works 100% or it doesn't work at all and that would really be the case where we would really see this being more ubiquitous, but as it stands there is a large degree of optionality across the board, which means that's really no true standard.

Christopher Bradley, MS – Chief Executive Officer – Mana Health

And, yeah, this is Chris speaking from Mana. You know I would agree that there is clearly still a lot of variability but I think the way we get to ubiquity of any one particular standard isn't necessarily by, you know, legislating it or requiring it but really having it be...creating value for all involved to have that

standard, have the fact that this standard is around...that the fact that the standard is around creates value. And I think if you look at other industries that have enabled widespread standard adoption by themselves without any type of, you know, government interaction they usually have done it because without that standard everyone loses.

So, I think as we start showing the potential for what having an API can really unlock for the patients, the health systems, the application vendors, the level of innovation, the speed of innovation I think a lot of the question of whether an API should exist at all goes away and then at that point it's really about some of the technologies and policies around an API that become a challenge.

Because, honestly, whether an API is identical from system-to-system isn't all that important as long as it follows some basic specifications but if we don't have common identifiers or patients, common practices and authentication of the patient identities, as has been mentioned, but also App identities, you know, authentication or sorry, authorization of consent for usage of data these are the types of questions that without a clear answer, universally, even if I have an API then I might interpret how to give access to that API completely differently.

And so as an application vendor now I have to figure out the policies and procedures, and legislation behind all of these things before I even start programming and distributing my application. And we feel, from our perspective that's really the challenge and that the value of an API in and of itself is going to be shown very quickly here as we start seeing, even in other industries, what's available and enabled by having that approach in terms of innovation and then quality of what's being done. So, I think that's something that we see and once we figure that out I think we're going to see extremely high adoption and I think a universal API is possible.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

This is John Moehrke. I totally agree with Chris. Fantastically said and, indeed, I think one of the things that really will drive that is to focus more on the 50% of the need than the 80% because you get up into 80% and you start getting into all kinds of various needs. So very focused on the bread and butter of what is needed.

I think driven, as Chris indicates, as a need and not a mandate will make a universal API happen. I don't think I see any other sustainable solution. Certainly customized APIs are not sustainable. Thank you.

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

John, I think...

Christopher Bradley, MS – Chief Executive Officer – Mana Health

I...

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

Just before...at this, you know, timing-wise from a privacy and security perspective and just want to try and figure out, is there a way that this particular layer, you know thinking about APIs as layers, can we picture a way of standardizing this that much of the privacy and security and the identity services are decoupled from the actual application and the user experience and so forth or are those un-separable.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

No, they...so, yeah, this is John Moehrke. I think you addressed that to me. Certainly, they are separable and they should be separated and the Security Workgroup within HL7 has worked hard to make sure that FHIR is being designed as an interaction model and a data model that is independent of the security model not because we don't think that there are good security models out there but exactly for this purpose in that there actually are very good security models out there, especially in HTTP, plus those...the security models can mature at their own pace for their own reasons independent of the data modeling efforts maturity that FHIR is going through. So, I very much encourage the separation of the security and privacy layers from the data modeling and interaction modeling layers.

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

And just to the guys who are product developers, is that something that the community can help lead and come to and decide on a product sort of a target to knock down and make a recommendation to ONC and others or how do you see the best way to make that something that's useful to you?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

So, again, this is John Moehrke.

Christopher Bradley, MS – Chief Executive Officer – Mana Health

Yeah.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Oh,...

Christopher Bradley, MS – Chief Executive Officer – Mana Health

Go ahead. Go ahead.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

That's one of the reasons why I am actively involved and advocating for the efforts that are going on with HEART it's not just a healthcare-focused group. HEART is an initiative run out of OpenID Connect with OAuth and UMA experts who have said, hey, we can help you with this and we just need to understand the healthcare certainties so we have healthcare people there, we have technology people and the IT security there. I think one of the things that is really missing is a realistic view and a simplified view of the policy problem that needs to be solved. So, it certainly needs more help. Thank you.

Christopher Bradley, MS – Chief Executive Officer – Mana Health

John, just quickly following up on...I really appreciate your comments about not trying to get to 80%, trying to get maybe to 50%. We haven't really, as a group, fully covered what we're trying to get out with these APIs. So, in your opinion what is the 50%, you know, what's the low hanging fruit that we can make a big impact with?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

I feel like I keep...so, I think guidance...so, some of the things that I've been involved in and one of the initiative we started at the HL7 committee a couple of weeks ago is to focus on document sharing, now I know, you know, many people will say documents are not FHIR, but the sharing of the documents and the manipulation of the documents accessibility to the documents can be facilitated by FHIR-based interactions.

So, we have a set of FHIR resources that are well-aligned with an XDS infrastructure so they could be backed by an XDS infrastructure but wouldn't need to be backed by it, it could be a direct FHIR-based API accessing documents.

Now that to me feels like a very focused thing it's the view, download and transfer functionality that's in Meaningful Use and it isolates really the clinical data within the document, which could actually be a FHIR-based document it doesn't have to be CDA, by the accessibility and indexing of those documents and it would include in there the harmonization of patient identities, the exposure of user authentication methodologies and the policies that would need to be addressed and include consent-based authorizations.

So, that would be my preference on what is the 50% is to really say, okay, can we at least get patient document reference and accessibility, and security of that available? And then we can move up to more fine-grained FHIR resources.

Christopher Bradley, MS – Chief Executive Officer – Mana Health

Thank you.

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

Leslie Kelly Hall?

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Thanks. I would just echo that our...the previous comments and also add that our minimum use case is really the common core dataset that we've defined in the current regulations. I mean, just getting that exposed and available to the ecosystem would provide tremendous value. And so we do have a smaller, even than 50%, we have a very specific defined case that we could use for both the provider and consumer's benefit.

Do you feel that this is a realistic and doable approach? And I've heard the comments for the Good Housekeeping Seal or having some sort of standards body but not regulation. It seems to me that we need standards body to manage but potentially regulation to enforce.

So, I'd like to hear your response to both the use case question and then with the...what you think the lines are between the standards organizations and the regulations to identify use?

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

Great question.

Christopher Bradley, MS – Chief Executive Officer – Mana Health

So, this is Chris from Mana speaking. So, I mean, in terms of...I think I understood the question, but in terms of where some of the benefits of regulation can come in, I mean, I think in some sense is, you know, getting access to the data itself is often difficult. So, you have a large, you know, body of people trying to solve, okay, how do I make this common core dataset usable through an API but if every time that happens there needs to be an argument for the value of allowing that to happen then that's just going to be slower.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Right.

Christopher Bradley, MS – Chief Executive Officer – Mana Health

So, I don't know...is that part of what you're asking or is that different?

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Yes, that is and then the first question was do you believe that the use case of just starting with what we already have in the Regs, the common dataset, would that be a useful approach?

Christopher Bradley, MS – Chief Executive Officer – Mana Health

I think personally, this is Chris speaking again, I think that it is. I think some of the challenges that we've encountered is the way of obtaining that data from the inpatient setting and in the inpatient setting those use cases tend to be somewhat different because there's a lot more information there, there's a lot more granular time attached to that information especially with say medications or procedures. So, I think those are more in the weeds issues, but generally speaking, being able to get to the common core and just figure out all the different needs around API use with that common core as a starting point could be very, very valuable.

And I'd say the first use case is, you know, mandating that everyone can actually give the common core out in any format but not blocking that access to that data I'd say would be a very important first step whether it's regulation or other incentives.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Thank you.

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)

Leslie asked the...almost verbatim question I was going to ask.

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

Okay, thank you. Josh Mandel?

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

Thanks. So, I wanted to touch on the distinction we've heard a little bit about how difficult it is to design standardized APIs for data and try to normalize the semantics of everything in the healthcare domain versus the problem of designing security protocols.

Now we've talked about how these are two separate things but I'm wondering if panelists could opine a little bit about the relative difficulty of these things and the relative priority that these deserve. So, you know, for example it's possible that focusing on having a common set of authorization protocols ahead of time, even if they're authorizing rather different data APIs under the hood or even if the semantics of the data aren't totally worked out. It's possible that working on the authorization stuff first would have a better sort cost-to-benefit ratio or maybe it's the other way around or maybe it's too early to tell but I'm curious whether the panelists have an opinion on those questions.

Christopher Bradley, MS – Chief Executive Officer – Mana Health

So, I...this is Chris speaking here again, I'm sorry, I'm speaking a lot here, but I'll be quick. I have actually a pretty, not strong opinion, but I do think that in a sense both are essential because for very narrow use cases you can separate out the two and security is very separate the API security is very separate from the data modeling and the semantic modeling. But when you start getting into more cross, enterprise, cross health system data use cases, especially with things that are getting, you know, a lot of excitement like population health and analytics, and machine learning, you know, these are all use cases that are going to require not just for the API itself to be secure but also a semantic and data modeling language that allows you to secure components of the dataset to allow very granular access to subsets of data and so I think that's where this combination of things has to happen where you need to be able to say what are some standards and to secure components of the record.

And then of course how do you then manage the access to those components in the right way for the right people and at the right time. So, I'd say that's where those two meet in ways that are actually very powerful but also quite challenging.

James Lloyd – Co-Founder & Chief Technology Officer - Redox Engine

Yeah, this is James, I totally agree with what Chris said, I think most of what we see is that this is actually beneficial to keep those two separated. And in many of the use cases for, you know, application developers as little healthcare specific information that needs to go into the security model is easier for the adoption side of things but, you know, the population health side that Chris mentioned is one but we also see, you know, specifically and also in the clinical trial space and things like that the need for sort of a healthcare specific and anonymization process and things like that that you have to go in an place and that's another area where it can start to blur. So, totally agree that they...that most of the time it can be kept separate but there are some use cases for definitely considering them together as well.

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

All right, thanks, very much.

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

Leslie Kelly Hall?

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

I'm set. Thank you.

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

Okay. A Josh it looks like you have another question?

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

I do. Thank you. I was interested in asking kind of an on the ground experience question for vendors who have worked with healthcare provider organizations to deploy Apps whether it's clinician-facing Apps or patient-facing Apps. My guess is that there is probably more experience on the clinician side up to this point in time but please correct me if that's wrong.

I would love to hear a little bit about the timeline between when an organization says “well, here’s an App we like, here’s a service that we learned about and we want to be able to integrate it.” You know how long does it take and in terms of that timeline how much of the time it takes is for things that fall into the general category of security review and certification testing, the kinds of things that, you know, we’ve talked about a lot on this panel and the last one.

And I’m wondering as well how the timeline differs. The first time an organization installs this App and then another organization comes along and they want to install the same App. How much savings is there that second time?

James Lloyd – Co-Founder & Chief Technology Officer - Redox Engine

Yeah, this is James. I can share some of our experience. And, yeah, so in general our experience has been around...it’s been around six to eight weeks from the time period of someone saying, all right, I want to use this, I’ll use an example of a telemedicine App, to the time that it’s wide and in the production. Most of that is going into the actual coordination of getting user reviews in place, so, you know, there are probably 10 or so check boxes that need to be filled by 10 different people at a health system for this to actually to happen and so a lot of it just logistics.

Often times there are two meetings, one to sort of set expectations and then one to do the final review on the security side. And then there’s also probably two weeks or so of technical infrastructure set up. And then we typically do two weeks or so of workflow-based testing and entity clinician sign-on and that kind of thing.

So, the pieces that actually go down in time from two and beyond are on the health system side actually for us rather than the application side. So, you know, an application goes to a second health system they’re going to have a brand new set of security check lists, a brand new set of contracts to go through that doesn’t reduce the time, but the second or third applications that a health system brings in, at least with us we’ve got a technical infrastructure in place and a sort of already established testing paradigm, so those are fewer discussions so that’s when it goes down to more of a 4-week type of time period.

Christopher Bradley, MS – Chief Executive Officer – Mana Health

This is Chris speaking for Mana. I would say what we’ve seen is the time it takes is actually very proportional to the size of the institutions as well as their maturity in deploying technology, which kind of makes sense.

So, in some cases, if it’s a very small practice with not many stakeholders and not many people involved in decision making it can be very, very quick. The technology becomes the rate limiting step and that could be, you know, as easily as a couple of days to go from getting some type of output to, you know, authorizing the application formally and then getting it up and running. But I’d say most of the use cases we’ve encountered it’s the opposite. And a part of that is because every organization has had to come up with its own set of policies, regulations internally to control access to this data because of the sensitivity of this data.

And so the larger the organization the more people usually are involved in giving access and authorizing access security making sure compliance is in line. So, you know, we feel like if there was a set of standards that an App can come to the table with saying we’ve passed x, y, z security review we’re compliant with these particular standards and we’re able to launch off of these types of APIs, as long as those are all agreed upon from an industry perspective and respected then really the decision making is

as simple as, you know, do you want this App or not and does it supply the needed value for the right, you know, price. So, I think that's why we're seeing that really is a rating limiting step and most of it's not technological at all.

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

Any other experience, Ted, on the McKesson side perhaps for App deployments?

Ted LeSueur, MS, CISSP, CHP, CSCS – Director, IT Regulatory & HIPAA Security Compliance - McKesson Corporation

This is Ted, yeah, I think what the panelists have stated makes a lot of sense. One other thought I would provide is that if you're looking at a standard installation of an application versus perhaps a hosted model that might provide some synergy around cost and timeframe. But, a lot of the process and procedures, policies, reviews, acceptance of the application, understanding what the application can do, how it's provisioned and authorized I think as the other panelists stated that's all very similar. Does that make sense?

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

Sure. Thank you.

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

Drew Schiller?

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

Yeah. Thanks, Michelle. So, I wanted to sort of go back to the conversation we were having this morning around the identity of a patient and get, from your perspective, from the panelists perspective from an IT background, what would be the challenges and potential solutions of, you know, identifying that as each of these patients are going, you know, from potentially from an App to, you know, any number of health systems, for the health system to know that this patient is who the patient says they are, you know, we don't have a universal medical ID in the United States and so, you know, what are your thoughts how we can ensure that we're identifying the right patients to access their data?

Christopher Bradley, MS – Chief Executive Officer – Mana Health

This is Chris speaking, I mean, I think that challenge what you just described is really two challenges is, can you authenticate someone's identity and then can you link that identity to the correct record or set of records around that identity.

And I think there's a lot of established ways to confirm an individual's identity that meets certain levels of standards that you can use for example in financial transactions and that are well established but without the existence of a universal medical ID of some sort to then attach an identity to I think that really becomes much more challenging.

And, you know, the industry has attempted various solutions but the error rates of those solutions of, you know, the master patient index approach, even if it's only several percentage points, presents problems at the level of scale that, you know, the United States encompasses where, you know, a single percentage point could be, you know, millions and millions, and millions of people that are mismatched.

So I think that's an open challenge and one that beyond access of data through an API is going to have to be solved in order for the data that is being accessed to be, you know, much more valuable. So that's what we see as one of the biggest challenges.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Well, this is John Moehrke, I would absolutely echo that. I do though want to bring in some other concerns. So, often times people just simply say "if we just had a national ID this problem would go away" and our experience...one example, is our experience in Saudi Arabia where because of the strong government they can have a national individual ID including anybody who is visiting. They still have this problem even though they have done as much as they can with the regulations and procedural to create a singular identity that is universal across all of Saudi Arabia for all purposes. They still end up...you end up needing to have some kind of mechanism to deal with the exceptions and they happen far more than you would expect.

So, I think we should do whatever we can to get our hands around it but we also have to be realistic and also get our hands around the realities that false negatives and false positives exist and root cause really should be driving what happens when those do happen rather than gross actions.

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

So, are you saying that we shouldn't let our concern over, you know, the fact that there will be likely errors we shouldn't let that stop us from moving forward? Is that what you're saying John?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

In essence, yes. That doesn't mean we don't put controls in place to detect and quickest react to it that gets to the incident detection and management I spoke of in my testimony. So, we always...what I'm trying to stress is that there is always risk. You need to manage the risk and to ignore the risk or to stop doing something because there is risk is not acceptable. So, yes, very much what you said, we need to recognize these risks, manage them to the best of our abilities and put in place mechanisms to detect failures and mechanisms to react to those failures appropriately.

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

John, do you think there's a way that we can engage the consumer in being part of that detection and correction?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Absolutely. I don't know what that is but we absolutely need to engage the consumers. They're usually...

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

Because they're always there.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

The one who will detect that. I'm a big fan of...

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

Thanks...

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

So, there you go.

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

No, I'm sorry, go ahead.

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

So...

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

I don't think...

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

Oh, sorry, go ahead, I'm sorry, I didn't realize there was more.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

No. I was just saying thank you.

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

Just one last thought before we move on from this, you know, there's...I mean we sort of mention other industries that are similar and one that keeps cropping up is finance and, you know, it seems to me like in the financial sector we have, you know, it's fairly straight forward for me to go and prove my identity to any number of financial institutions and credit bureaus and, you know, whatever. So, why is it so much more difficult in healthcare than it is in other industries to...for people to know that I am who I say I am?

Christopher Bradley, MS – Chief Executive Officer – Mana Health

This is Chris speaking. I mean, I actually would argue in a sense it's not that...that's not the difficult part because we just leverage the same standards the finance industry uses through challenge questions and other means and then at least we solve that question at a level of assurance that's used elsewhere for sensitive data.

So, I'd say, you know, healthcare in a sense doesn't need to reinvent that wheel or resolve that problem but the challenge then comes to linking that identity to the rest of the data as we've been, you know, speaking about and I actually that this shouldn't stop us from, you know, continuing to establish use cases for APIs and for how to do this in the medium term but I think in the long-term that's just an open challenge that has to be solved and I don't think anyone's been able to solve it yet.

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

One of the things that I've observed in the finance space is before I create an account or anything they ask me identifying information in a standard way so that it can actually assign and use an identity. We don't seem to have that practice in healthcare that might help.

Christopher Bradley, MS – Chief Executive Officer – Mana Health

Yeah, good point...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

And...

Christopher Bradley, MS – Chief Executive Officer – Mana Health

One key difference here between sort of the, you know, financial, you know, Experian, kind of experience is that there's a sort of central repository, at least in the US, where the data for the questions are coming from where, you know, if we were to generate a set of challenge questions in healthcare I think that one of the questions would be what are we comparing that to and where is that...ultimately, what's the repository from which we're generating the questions and answers from?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Yeah, the other difference in finance is accounts are revocable, exposure of personal medical information is not revocable.

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

Right.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

I do want to point out there are some sites that are using identity and assurance elevation through starting with low assurance identities and elevating the assurance through various means. And some like this, which are asking qualifying questions, others which are doing in person proofing to elevate a lower quality identity to a higher quality identity. Some of those are seemingly to be accepted by the consumers.

So, many consumers want to use the identities that they already have and already use often. One reason is they're familiar with them and it's easier for them to detect when those identities are not being used properly.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

This is Leslie, there has also not been any reason to avoid duplication when there have been systems that have not been connected.

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

Great point.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

And when there's no penalty for lack of payment when the patient isn't identified correctly back to the payer for instance so there's a new account generated with every visit so it becomes more difficult if every time I visited Wells Fargo I was issued a new account, it becomes very difficult to manage those connection points.

So, some of our workflow, historical workflow, contributes to this lack of connection. But to the earlier point, Aaron's point, when we present to an institution with our identity and we have the ability to create then a certificate or access to the portal that you have at least that first step in our current workflow. It's been...

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

Before any data is generated about me.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

How do you stand upon that.

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

Yeah.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Yeah, right.

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

Exactly.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

So, that becomes something we could leverage. The...I think that the other issue with banking is that the record is the banks and I cannot contribute to my record in that I can't tell them, you know, that balance is wrong you've done the math incorrectly or I don't get a lot of flexibility to change the record and the absolute truth of the numbers is generally the banks, 90% of the time, and so I can edit by how I spend and how I report on it but I can't change that stat and so we're a little bit more complex in healthcare because that record is somethings that is much more more fluid and the patient has the right to provide information back and ask that information to be included into the record for corrections or errors, or just simply for better health because it is the patient who has the ultimate risk of harm.

We can talk about the data breaches, we can, we can talk about all the data issues but it is the patient's health that presents the biggest risk. And so in the banking industry it's not...the incentives are the bank holding the risk and not necessarily the individual user.

So, there are things we can learn from that but there are other things that we need to keep in mind that we have to protect....we have to protect the patient but also make the patient available to use their data in any way that they choose.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Well said.

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

Coolness.

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

Yeah, than panelists for sharing with us their experience I've really enjoyed listening to the discussion. My question is, we were reminded in the first panel today to consider resources of small providers from both a technical and compliance perspective. So this is open to any of you if you would mind describing how your business model supports these providers and what some of those challenges look like that we should keep in mind?

Christopher Bradley, MS – Chief Executive Officer – Mana Health

This is Chris speaking. So, I mean, you know, what's interesting about your question is in a sense if we succeed with some of the challenges that we're describing and there is a standards-based API approach to data access that would drastically lower the barriers to enabling these services very cheaply and

quickly. And so any type of financial barrier or financial constraint that a smaller provider would have or a technical sophistication constraint that they may have is no longer an issue.

And I think the best example of where this works extremely well is on your phone. I as a consumer of applications don't need to know anything at all about how it works to launch any number of applications on my phone regardless of platform and I think that's ultimately the success of standardizing and optimizing the way technologies interact is that sophistication of the user can be very little to none.

So, for us, you know, in a sense, by working on these problems both as a private entity and also as a larger public effort such as this one the real goal is to enable these smaller providers and practices to benefit from the innovation that they often sorely need.

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

You know one of the differences though I think...or could you speak to this Chris, you know, with phones there's like two to three platforms. With practices, you know, even if they're using the same EMR vendor the actual...at least the data in some of the customizable UI is different from practice-to-practice.

Christopher Bradley, MS – Chief Executive Officer – Mana Health

Yeah, I think that's valid. I'd say the metaphor breaks down at that point but I would say, if in a sense the API approach aims to nullify that issue because the API will be the same despite, you know, vast differences and approaches to data storage and technologies used so...

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

Yeah, right.

Christopher Bradley, MS – Chief Executive Officer – Mana Health

Ultimately what that enables is that type of simplicity even though, yeah, I completely agree it's three to four platforms versus hundreds and hundreds is definitely your challenge.

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

I hear you though about...you know if we were all to use the same FHIR resource standards you could at least expect when somebody says they're sending you the EOB equivalent that that's what you're getting from the payer.

Christopher Bradley, MS – Chief Executive Officer – Mana Health

That's right, exactly.

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

Yes, yes.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Yeah, this is John, I would agree with Chris, using standards driving towards standards, driving towards focused solutions is what eliminates overhead. Eliminating overhead eliminates cost so that's what we...that's why we are very standards focused.

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

Just a realistic expectation is that it's not going to be as trivial as Google Play or Apple Store for healthcare but actually, you know, there will be savings and the more we standardize the better off we'll all be.

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

This is Michelle, it looks like we don't have any other questions in the queue from our Task Force members so let me just see if there's any Task Force members who have additional questions?

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

I just wanted to try and...there's a third question that we asked the panelists before today which was, what are the perceived privacy concerns, like...do you hear from your customers or your customer's customers, i.e., patients, are there perceived concerns at this point? Is that something that's reaching your product development lifecycle about privacy concerns or are we projecting some of this?

Christopher Bradley, MS – Chief Executive Officer – Mana Health

So, this is Chris speaking. I think that's a really interesting question about, you know, are there concerns versus is there actually, you know, really a privacy issue and I would say it's interesting, depending on the groups that you interact with. From-an institutional perspective there are always concerns just generally because it is their data but it's also not their data and there's a lot of regulation around what happens if that data is accidentally exposed so there's a lot of concern.

And at the patient level I think there is concern in some cases but in many, many cases when we've interacted with patients as part of our patient portal development work the vast major of cases we've heard that privacy is a concern but not as big a concern as their providers and care team not having all of their information when they need it. So, I think that was very interesting for us and I think it came up in the previous panel...

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

Right.

Christopher Bradley, MS – Chief Executive Officer – Mana Health

In doing no harm, you know, does it really...is there less harm to be done by worrying less about privacy than access to data for the right people.

James Lloyd – Co-Founder & Chief Technology Officer - Redox Engine

Yeah, this is James...

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

There is...

James Lloyd – Co-Founder & Chief Technology Officer - Redox Engine

I think we need to appreciate that there is also a spectrum of types of users and I think there will be some folks who are very comfortable in trading off a little bit of privacy for additional functionality and convenience while there will be other folks who say, you know, I really want to have full control of that and, you know, these sort of features that, you know, if you go back to the phone analogy, you know, I can have location services turned on and get a lot of benefit out of that or if I don't want, you know, my

location always being tracked by my phone provider I can turn that off and I think, you know, we need to sort of look at this as not sort of a one-size-fit-all type solution but one where there might be different types of consumers who want different types of features and functionality.

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

Ted you mentioned at the beginning of your testimony that you had put together, you know, something that you use at McKesson sort of internally. Does it reflect a spectrum of preferences or how did you guys approach it?

Ted LeSueur, MS, CISSP, CHP, CSCS – Director, IT Regulatory & HIPAA Security Compliance - McKesson Corporation

This is Ted and yes, I would say that it does reflect some of those...some of that feedback that we receive. A lot of times that can be part of the configuration as we're implementing the giving solution for our customer. But often times, you know, I think that there is...what's the best way to say it, maybe that the request from the customers of our customers are patients, right?

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

Yes.

Ted LeSueur, MS, CISSP, CHP, CSCS – Director, IT Regulatory & HIPAA Security Compliance - McKesson Corporation

Versus what our actual customers want that can be kind of different. And so, I think, you know, one of the things that has always impressed me is that when you look at the everyday user, the everyday patient, and ask them how important is your health data, what do you believe we should and should not be doing with your health data? I think that's a very a different response than you might receive from an institutional perspective and I think that's where some of this conversation comes about in the earlier question about, you know, maybe are we projecting privacy concerns where maybe there aren't as many as we think there are?

Boy, I think that's a great question and I'm not sure that we have a clear and defined answer on that. I think, you know, what was also said about one person really wanting to ratchet up their privacy capabilities and another person saying "no, I'm good" to use the metaphor analogy that "yeah, I'm going to turn on location services not a big deal to me." I think all of that really plays in and until we...as I said in my statement, until we come to the trust framework that's unilaterally adopted, boy, I think we will struggle.

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

Thank you for your testimony, everyone.

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

It looks like Leslie has a question.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Yeah, thanks, I just...I've worked with a medical ethicist for a while and used to ask the question, take things to its logical, natural conclusion and then design to that. So if we were to say that we had interoperability using APIs where there was the ability to take data and move it around to all of the

ecosystems, who do you think should be responsible for that privacy of that data and control of that data?

And I would pose that in that scenario, it's likely the patient and not the provider. The provider is the steward of the day-to-day hold but not the steward of the data that moves. And so if that were the case and the patient is that ultimate controller of the movement of data, what do we design differently today?

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

Hi, this is John. I think if you look at it with logic I think you will come to that conclusion that logically the patient is the one who has the most stake in appropriate use of the data and preventing inappropriate use of the data. I think though that there are two forces that have to also be recognized at the very same time, one of them is just momentum.

We have the system we have, we just...I mean, no one would have designed the system we have knowing, you know, where we needed to go but we have the system that we have and it's highly decentralized, it's highly focused on the reasons it has to exist.

But the other one is, I really think this question and the previous question have to recognize that the largest majority of individuals want to just trust the healthcare system to do the right thing for them.

There is absolutely a need and desire by a group of people who I don't want to diminish, but is smaller than the larger masses that is...that absolutely needs, as I said, the ability to control their data and want the ability to control their data, but I just, you know, want to put it out there that I think the vast majority of individuals really just want the system to work for them and they don't want to think about it.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

You know that might have been true in the past and I would challenge that now. The National Partnership did a great study on how people use the data. We're seeing all kinds of examples, I think today or yesterday there was a study out that said people over 65 who have access to their portal are using it on an average of 39 times a year so I think there is a demand.

I would also pose that when things are opaque or information is not available we all have to think that everything is going well because without that kind of confidence the system breaks down. When things are transparent and open we begin to see how as individuals we can correct and help, and promote, and progress our own cause because of that transparency.

So, today we're trying to manage a void it's impossible. Once we have that void opened up and people available I think things will change.

Christopher Bradley, MS – Chief Executive Officer – Mana Health

Yeah...

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

From an accessibility use I very much agree people will respond to they want to use their data I was just addressing the control question, do they really want to participate in controlling?

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

I can give you a small example...

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

But I acknowledge...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Of my...

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

I acknowledge your thinking.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

You know my 94-year-old mother who went to the doctor asked for the record and saw that she had records from at least six other Helen Kelly's combined in hers and started to figure out, well, how do I go and get the data and move it and why don't I know what data is moving because I could have told them I'm not that Helen Kelly. So, again, when things are open and we begin to see errors. So, thank you very much for your testimony and your point-of-view, appreciate it.

John Moehrke – Principal Engineer, Interoperability & Security – GE Healthcare

I do want to stress I agree with that point though. I also have plenty of examples on that point, accessibility and transparency absolutely agree.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Thank you.

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

Okay, thank you everyone we appreciate all of the time that everyone spent on Panel 4. I think we're going to transition now to Panel 5 but before we do that we're going to take a quick five-minute break and during that time, I'll make sure that we have our panelists for Panel 5. So, we'll regroup again at 2:30 and again if you step away please just mute your phone. So, I know we're on break but let me just do a quick check.

At the break we had all of our panelists so just a reminder to all of our panelists, you have five minutes for your presentation, hopefully I won't have to ask you to wrap things up and with that I'm going to turn it over to Adrian.

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

Thank you. I'm Adrian Gropper, Chief Technology Officer at Patient Privacy Rights. Patient Privacy Rights is the world's leading 501(c)3 not-for-profit health privacy advocacy organization. We represent a bipartisan coalition of 50 US organizations with 10.5 million members and 50,000 members of our own.

Patient Privacy Rights mission is to restore patient control over personal health information. To accomplish our mission we educate and work collaboratively with patients and organizations to restore the ethical rights of health information privacy the foundation of the patient/physician relationship in law, policy and technology. I'm a medical software entrepreneur by trade, have contributed to a number of healthcare standards and a Co-Founder of the HEART Workgroup.

Patient Privacy Rights would like to address a gap in the system we have today that makes it difficult for health records to follow the patient for second opinions, cost-effective treatment alternatives and from donating health data for research and other uses.

PPR would like to make five points, that a distinction between the patient-facing API and the FHIR API is unnecessary and undesirable. It is the right for the API exposed to the patient or it is illegal for the API that's exposed to the patient to be different.

HIPAA explicitly allows the patient to delegate access, direct access to their records and lab results that includes access to second opinions by the licensed professional of her choice. With very limited exceptions HIPAA says that the data that's accessible via other means will also be available through a patient-controlled API.

Point number four, the HIPAA Security Rule, as applied to FHIR or to a patient controlled API, could be used for data blocking by institutions. Data holders that use security arguments to justify blocking patient's specified FHIR Apps or clients are violating the law.

And finally, number five, potential security gaps can be fixed by appropriate protection design of UMA, HEART and FHIR so that the unified public API does not force a compromise between privacy and security.

The JASON Report and Task Force laid the foundation for the public API. We must leverage the market forces behind FHIR and Argonaut to also improve access by patient directed third-parties. As the recent OCR guidance makes clear HIPAA gives the patient the right to have their health records and lab test results sent directly to a third-party even one that may be consider insecure or unwise by the covered entity or data holder. Paternalism is not legal.

Unfortunately, the current guidance can force the patient into accepting an insecure transfer method such as an unencrypted e-mail or the use of slower and less reliable methods such as the Direct e-mail attachment.

A unified FHIR-based public API should not force patients to choose between privacy, which is control over uses of PHI, and security. At the patient level the content of a FHIR API for providers and patients is substantially the same. Patient safety requires that clinicians are able to bypass policy based delays on the patient directed API. Patients expect real-time access.

Data blocking will continue as long as covered entities and health data holders control which APIs or clients are safe under the HIPAA Security Rule, FHIR, HEART and this Task Force must end the paternalistic illegal blocking of patient access to EHR data and lab test results.

The OAuth privacy and security technology underlying FHIR and HEART is the best solution for patients and industry as discussed in the Joint HIT Committee, a patient specified third-party web service destination cannot be blocked on account of HIPAA Security grounds.

FHIR and HEART should be harmonized to enable a public API by applying privacy engineering now while the standard is still immature. PPR welcomes the opportunity to work with industry, government and providers to ensure the data follows the patient without compromising data security. Thank you.

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

Thanks, Adrian. Mark Savage?

Mark Savage, JD – Director of Health Information & Technology Policy & Programs – National Partnership for Women & Families

Thank you very much for the invitation to be with you today. If you could go to the next slide, please? So, I'm Mark Savage, I'm the Director of the National Partnership's Health IT Team and I'll be sharing today views of the National Partnership for Women and Families and the Consumer Partnership for eHealth, a national coalition we convene, have expressed in recent comment letters to CMS and to ONC. Next slide, please.

In those comments the consumer partnership has observed that in many ways consumers and patients are look at underlying needs, functions and uses not necessarily the technology that provides them. They expect important functionalities through online access and portals and as we're now moving to APIs they also expect those same functionalities at a minimum through APIs. It may be better, it may be more usable, more useful and more innovative but still want them to be available.

So, we have recommended that it's important to keep online access and APIs both available for now to make sure that consumers and patients have all expected functions and you see there some of the functions that we have lifted up, online access, being able to share patient generated health data and non-clinical data, sending secure messages, even the convenience features of requesting appointments and medication refills.

We also made the point that the 2015 edition requires APIs to provide access to the common clinical dataset but we note that consumers want access to other key health data as well especially in areas like care planning, referral summaries, discharge instructions. These are things that are really important, really helpful in care. So, a suggestion that we broaden the access through APIs. Next slide, please.

The concerned partnership has also shared some important views on privacy and security issues with APIs. Because there are significant privacy and security implications especially with APIs HIPAA's privacy and security protections do not apply to many commercial Apps and personal health records unless provided by HIPAA covered entities such as providers, payers or their business associates and consequently many applications and devices may have, for privacy policies, weak security controls or policies that share data liberally with third-parties without...perhaps without the patient's knowledge at the time.

Many consumers may not understand this at all or may have limited understanding of how privacy and security protections change or even end when they move data from their HIPAA covered entity to a third-party application or device. So, we think it is critical to protect against such surprises in order to preserve and build consumer trust for the long haul. Next slide, please.

So, we made some recommendations to help and these are recommendations that reach providers, developers, and consumers alike. First, we recommend that ONC, OCR and CMS should collaborate on ways to educate consumer about their rights and steps that consumers should take to protect their data, examining policy options that improve privacy and security for patients using Apps and APIs to download and use their data.

Second, ONC and OCR, and CMS should also educate providers who are likely to receive questions from patients and family members about APIs such as what they mean, how they work and are they safe. This is additionally important because doctors are such a trusted source of guidance for patients. And I would point out that OCRs recent guidance on access is a great example and I understand that there's more to come.

Third, API and application developers must communicate their privacy policies clearly in plain language to patients and consumers, as well as providers. Indeed we encourage technology vendors and providers to partner with patients and families to develop and communicate that important information about APIs. Next slide, please.

The National Partnership also coordinates the new Get My Health Data Campaign and here we've collected some more specific information about Apps and APIs. The campaign advocates for policies, technologies and other solutions that enable consumer health data, download and use to become the norm and we coordinate that with other leading partners. Next slide, please.

So, here you see a summary of some of the key pieces of information that the campaign publishes because this is what consumers want to know. They want to know about transparencies so that they can make meaningful choices about APIs and PHRs that meet their needs. The consumer...the Get My Health Data Campaign will not list Apps and PHRs that release identifiable health data without the patient's explicit consent because that transparency is so important.

Second, privacy notices can be opaque and so the campaign asks whether the vendor uses ONCs model privacy notice.

Third, many consumers want to be able to download their health information to use it.

And lastly, they...the campaign asks about whether the App offers the use of a secure Direct e-mail address not because that's a critical...the Direct e-mail address is the critical way to do it, different patients want varying levels of security and flexibility in their e-mail and this table just discloses whether the option is available. Next slide, please.

This captures a little more detail about what consumers want to know about Apps and APIs and you'll see that the list here affirms much of what the consumer partnership has said in its own comments both in how they want to use it and in the data from the different sources that they want to be able to incorporate through Apps and APIs. Next slide, please.

I would like to close with an even broader consumer view. A year ago the National Partnership published our second nationwide survey of how consumers value and use health IT. The Harris poll conducted it for us it's weighted to be demographically representative of the total US population.

Interestingly, we found, from our first survey in 2011, that online access had doubled from 26% to 50% in 2014 and of those with online access 86% used it at least once per year, 55% used it at least three or more times in the last year.

So we asked...one of the things that we asked respondents was whether they had accessed their medical or health information through a mobile device and whether they would like to have that capability and

this chart gives you the responses by different demographic characteristics because some communities are actually making greater use of smart phones than others in order to help bridge digital divides.

Interestingly, Hispanic, African-American and Asian-American patients were significantly more likely to have used a smart phone or tablet to access their health information and Hispanic, Asian-American and LGBT individuals were significantly more likely to want to use mobile access. And on the right you can see the significant numbers of people who are already using a smart phone or tablet for access and this gives some hints about the use already in place of APIs. Next slide, please.

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

Mark, can you please wrap up? I'm sorry.

Mark Savage, JD – Director of Health Information & Technology Policy & Programs – National Partnership for Women & Families

That's okay. Thanks so much. Lastly, using APIs for what, this is...we asked them what they...what features they wanted to use and this gives you the responses of which features they found most important. I'd just note that these are sort of the features that have already been developed so as developers are developing new features this list may change that's the importance of innovation. Thanks so very much for your time.

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

Thanks, Mark. And finally, Steven Keating?

Steven Keating – Patient Advocate/Consumer – Doctoral Candidate, Mechanical Engineering, MIT Media Labs

Hi, great, thanks so much for the opportunity to present and for the person that's clicking through the slides I have a lot of them so feel free to just cruise through as we go. So, I'm a current PhD student at MIT and I'm speaking today on the patient perspective as I'm currently in a personal brain cancer situation.

So, I thought I'd start out with some statistics. People are throwing more and more data online these days. For example there's over 650 billion photos uploaded per year. And well, what do we do with all that data that we're sharing, well we can use it with Apps.

So, if we look at, for example, the iPhone there's over 1.5 million Apps available and the average price is actually only 19 cents and 90% are free. So, then the free market can actually have usable tools they found ways to incentivize and create Apps that generate capital without charging the consumer. And what is the result? Well, look at for example, Wikipedia the world's largest encyclopedia by a huge factor and it's created by all for all, right? So, how come healthcare hasn't caught up to this?

I was absolutely shocked as a patient to realize that they're still using fax machines, they are mailing CDs with data on it. They are constraining patient portals, right? You're stuck in one portal that you can't really do much with the data. There are no tools and there are no standards for switching between hospitals. There are legal gray zones everywhere. For example, I still don't have access to my own brain tumor genome, my doctors and researchers do, but I still don't.

And, you know, on the legal gray zone side with data who actually has copyright over it? So, for example, my surgery was videotaped, do I need all the permission of every doctor in that video for me to publish it online or share it or can I use it for fair use, right?

And finally, there's no translucency so there's no map for a patient to figure out what hospital to go to, what treatments to look at or to share their own patient experience.

And so the reason I'm talking about this is access to my own data from a research study actually helped save my own life. So, I've always been curious and in fact in 2007 I actually volunteered for a brain scan and I asked for the data back and it actually showed a small abnormality and they didn't know what it was so I got it re-checked in 2000 and 2010, no change. I kind of went about my life but I had access to the data and led me to ask for another scan in 2014 when I smelled a very faint vinegar smell that I knew that the abnormality was near the smell center.

It was three weeks later I had this large brain cancer tumor cut out of my head and I tried to access as much data as I could to visualize it in different ways. So, for example, you know, looking at 3D printing of the tumor and 3D printing of my skull. I think we're a couple of slides back if you just want to catch up.

So, you know, how come more patients can't do this? How come we can't leverage our own curiosity, right? How come you can't have an iPhone App where you can...instead of being scared or bored in an x-ray machine you can actually access your data and 3D print a version of your brain tumor and give it away as Christmas tree ornaments, right? Or you can see your own pathology. So if you look at the cell's tissue, if you keep advancing a couple more slides, you can actually...you know you can download a PDF that changes your biology textbook to use images of yourself, right?

And if you actually go even another step further, if we gather data from outside the hospital, such as microbiome and your Fitbit data how come we can't integrate that into the healthcare system and into the research field, right?

So, to give you some context, I tried to gather as much data as I could about myself and it totaled over 200 gigabits of data, right? And so how do we actually use that data? Why don't we have tools like a Google maps or a Facebook, or a Dropbox for health, right? I couldn't find any of those tools so I ended up putting all the data online and this was for friends and family on my own website and when I was talking about it I got contacted by numerous patients and they wanted to do the same thing.

So, why can't we leverage curiosity? Why can't we encourage people to share even only if 0.01% of Facebook users contributed data, if there was a share button for medical data on Facebook it would be one of the largest medical studies ever conducted, right?

And if you look at Apple's Research Kit you can see that when the tools are simple people will use it and they will share. And if you look at OpenNotes you can see that patients care about this, that 70% have reported taking better care of themselves with access to their doctor's notes. And we can enable this all through an open API under patient control.

So, to summarize, I wanted to focus on five points for APIs moving forward. We need to make sure they're simple to use, we need them standardized, open to third-parties, we need it to be patient controlled with full access to the raw data, and I think this is an important point here, we need to differentiate between raw data and analysis, right? Right now they're kind of grouped together so every

study of people...a person participates in has to go through IRB review if the patient gets any results back. We need to separate that, there definitely is a raw data that shouldn't require IRB review and then there is analysis which should require IRB review to make sure that you're getting back quality analysis, right?

So, we need to enable it to make sure these APIs can handle research data and patient submitted data and keep raw data isolated from analysis. And so, I'd love to wrap up now and if you just want to go to the last slide, oh, yeah, perfect.

So, I wanted to say that the most important thing is we need the general public to realize that support itself is medicine and by having access to the data and to use it we can generate support. So we need to fund more research around quantifying the effects of what the sharing medical data does. What is the value of this API?

We need to have tools ready so that when these APIs come out we can hit the ground running and make sure patients are driving the change.

So, with that I'd like to wrap up and you can also note that I added a few more slides at the end with long text in case want to see more depth and for example you want to see examples of other APIs in the healthcare field that have been successful and ways to think about ensuring standardization works. So, thank you for your time.

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

Thank you, Steven and thank you to all our panelists on Panel 5. Aaron Seib has a question?

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

Amazing testimony, thank you to everyone. You know one thing that kind of resonated in my mind with Mark's presentation and with what Adrian shared, and especially with what Steven shared, we talked a lot about the patient's right to access and some other thoughts. And, you know, one of the things that I think we have as a right is to have our data sent to us via any method including insecure e-mail.

I'm just curious if you guys can sort of voice for me your thoughts on the importance of that right, how do we preserve it or is part of the education that we need to do that there are some risks associated with that and make sure people don't become dependent on insecure means of exchanging their data or is that also being paternalistic?

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

Well...

Steven Keating – Patient Advocate/Consumer – Doctoral Candidate, Mechanical Engineering, MIT Media Labs

Yeah, I have to jump in here...I totally am a very big supporter of the idea that there should be patient variability so that the choice should be given to the patient with what they want to share, if they want to share and to be able to accept responsibility and take those liabilities into account.

And I think a nice example of that is, if you look at the Personal Genome Project, and as a disclosure, I'm one of the board members of the Personal Genome Project, it's a site where you can contribute your

genome and share it with the world for research purpose and in order to do that you actually have to pass a test which makes sure that the person contributing their genome online understands the liabilities.

So, you actually have to read through and you have to say, I understand that in the future we don't really necessarily know what will be able to happen but, you know, you could be cloned or, you know, maybe someone could develop a virus custom to your DNA, right? These are long shot, you know, possibilities but that test is to make sure that the person who is submitting to share their data online for their genome understands those responsibilities. So, I think it's very important that we ensure that this flexibility is there that we are not always designing these policies for the worst case scenario because that's currently what's happening.

If you look at the new common law proposal there's actually a de-incentivization to give patients back their data because they're worried they might hurt themselves with it. So, you can actually for secondary research, one of the new proposed criteria in the common law, is that if secondary research has no risk to the patient and patients are forbidden to access the data coming out they don't require IRB review. And to me that's completely the opposite of what Obama's pushing with precision medicine.

Instead we should be able to have a designated record set of raw data that doesn't require IRB review. I'm not talking about the analysis, I'm separating the analysis from the raw data. Analysis, yes, should definitely have IRB review and that can be done by hospitals and things like that, but patients should always have access to that raw data and be able to make the decisions they want and accept those liabilities.

So, I think a nice medical word is computer programming, right? For probably most of you and for me too I'm not going to into my computer and get down to the source code but I could if I wanted to it's legal, it's fine for me to do that. For those who are adventurous and want to do that you can go down and develop new programs and Apps and that enables the rest of the population to use those Apps with their own data.

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

Thanks.

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

This is...

Mark Savage, JD – Director of Health Information & Technology Policy & Programs – National Partnership for Women & Families

This is Mark, I would add to that, what we're hearing from consumers is that they want that variability and the one new piece is the...therefore the importance of transparency about what is being done so that they can't...so that different people can make different...can make choices that are appropriate to their different preferences. They'll know if it's secure or not or if there are varying levels of security they'll know how secure it is.

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

The...

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

Aaron Seib, this is Aaron Miri, you know, let me use an analogy here, if you go to your bank and you get your bank statement for the past month and you find a whole section of it blanked out they're not going to give it to you and say "oh, we made these decisions and charged you these fees" but they don't tell you what it is, you just know you got something deducted from you, would you be good with that? Probably not and that's the way I look at it as in we have to be completely transparent and give back to the patients whatever they require, their own record, as well as I agree with that attestation aspect, they understand the risks and whatnot, but, I mean we have got to get beyond this data is control, control is power. We've got to get beyond that.

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

There's another perspective on this which we heard in the previous two panels a lot of discussion about the relationship between the EHR's vendors control over an App or the authorization of an App and the hospitals or the providers control over Apps and authorization, and I submit to you that the licensed physician needs to be able to trump vendor and institutional blocks.

We always used to have this ability to introduce the licensed provider, as a...you know as an arbitrator of, you know, exceptions and issues and this has been lost and this was not lost on my medical society where we passed two resolutions particularly around the time when Direct, you know, Direct secure e-mail was coming into use about sort of this gap that had opened up.

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

So, this is the question I raised yesterday about consumer education, how...when do we know that the consumer has made an informed choice? How do we educate them to the degree that we...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

When the patient says they've made an informed choice.

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

Okay.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

It can't be...it can't be when someone else deems it informing for them. What we can do is provide the information it's like leading a horse to water, right?

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

Yes.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

So, we can be thoughtful on that but we certainly can't deem whether or not the patient is capable to use the data. They recognize the terms of service...

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

Informed about the risk.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Hopefully we've done good education, right?

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

Right.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Identified the risks but...

Mark Savage, JD – Director of Health Information & Technology Policy & Programs – National Partnership for Women & Families

And this is Mark, I'd point...that's one of the reasons why I mentioned the recommendation about developers and providers working with patients and families because you can make some assessment ahead of time about whether something is completely inscrutable and is not going to be of any use and with the goal of trying to make this transparent and understandable to patients and families. And then when they do exercise their choice we can have confidence that their choice is an informed one.

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

That makes a lot of sense to me. Thank you.

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

Josh Mandel?

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

Thanks, so first of all, thanks again to the panel for really an excellent set of presentations that lays out some important issues and also provides quite a different perspective than I think we've heard in the last series of panels.

For me I'm very interested in the diversity that we've identified which is to say that healthcare consumers come at the question of accessing their data from many different backgrounds and so for some consumers what they really want is to make sure that the tool or the App they've chosen is safe for them to use and it's going to protect their data in reasonable ways, and then other consumers are actually the ones writing the Apps and, you know, there are...because they're writing it themselves they're taking their data into their own hands.

And the question is, how can we foster an ecosystem where this whole spectrum of consumers has access to the kinds of protections they need. The thing I'm worried about is if we set up a system of certification programs like the ones that we've talked about quite a bit in these panels where organizations will go through multipoint checks and ensure that applications are adhering to security practices and go through a complete review. If we set all of these things up then it seems to me that the individual who wants to write their own App for open source purposes is going to have a hard time jumping through those hurdles and going through a six-month, you know, multi-thousand dollar review process it just won't be possible.

So, how can we give provider organizations a way to share data in a fashion that's appropriate to this whole spectrum and still protect the consumers who may genuinely want that degree of protection without interfering with those other cases.

Steven Keating – Patient Advocate/Consumer – Doctoral Candidate, Mechanical Engineering, MIT Media Labs

Yeah, I'm happy to jump on this, this is Steven Keating here, so I completely agree with your analysis that there is a huge variability and we need to enable it across the spectrum, right, we can't just...that's been the problem with HIPAA and CLIA, and the new common rules they're always...they're always written for the worse-case scenario and they're not able to have that variability which is really important.

So, I think your question is very appropriate and what I would suggest is similar to the way that Apple, you know, runs the App Store where there is verification of Apps, right? So, for example you could go...if you're very cautious about your safety and stuff you could have your hospital or go to a trusted medical source that approves Apps and only use those Apps, right?

But, because through an API the patient should be able to send their data to any third-party just because the recommended Apps, which are available through the hospitals and, you know, the health stores that will pop up through medical certification programs, doesn't mean that you can't experiment and send your data to, you know, experimental Apps.

And I think a nice paradigm for this is, you know, and I mean this is a little bit crazy to think about, but you can jailbreak your iPhone and you can actually install any program you want once your iPhone is jail broken you don't need to have approval from the App Store you can actually...and there's a whole amount of Apps out there that you can push your phones to do novel interesting things but you are taking a risk because that App has not approved by the App Store. And the same thing should be able to happen for health.

And I think it's...as a PhD student at MIT I'm always seeing these health hack-a-thons where you have the teams of these amazing students who want to create the next generation of medical Apps but they get stopped every time because of the regulations for data access and it's a real problem because the patients are on the other sides saying, we want to try out these experimental methods especially for people in really dire circumstances they're okay with sharing their genome, they're okay with sharing all this stuff because they're in a critical situation and if they are understanding the liabilities they're taking they shouldn't be restricted to just those approved Apps.

So, I think having that variability in the kind of two-tiered model where you have Apps that are approved by, you know, a hospital and the hospital's official policy could be, you know, for patients we recommend only using these set of Apps that we've approved, but because it's an API you can have Apps developed by external parties that don't require certification and it's just like taking your data out of HIPAA once you do that it's yours and you can send it wherever you want.

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

So, I really want to hear from the other panelists as well but I want to ask a quick follow up question to Steven if I could.

Steven Keating – Patient Advocate/Consumer – Doctoral Candidate, Mechanical Engineering, MIT Media Labs

Sure.

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

Which is how do you envision this playing out as a user experience. In other words, if I'm going to approve an App that, you know, maybe has no certification and that my hospital doesn't trust. When you jailbreak your iPhone you're not doing that with Apple's blessing...

Steven Keating – Patient Advocate/Consumer – Doctoral Candidate, Mechanical Engineering, MIT Media Labs

Right.

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

You're doing that because you're taking the decision into your own hands and you have the full capability to do it, you've got the hardware and you own it. But when it comes to getting your health care provider organization to open up the data access you actually need their help to open it up.

Steven Keating – Patient Advocate/Consumer – Doctoral Candidate, Mechanical Engineering, MIT Media Labs

Right so that's where hopefully a standardized open API and/or patient control comes in. So the hospitals can't limit you to do that, right? So, it's just, you know, for example, right now, take 23andMe as an example, so you can submit your cheek swab to 23andMe pay your \$200.00 and you get back the data and the results from 23andMe and they'll give you their own analysis, right? And for most people that's totally fine that's all they want, they can view the analysis and it would be just like using an approved App at the hospital. But for people who are more adventurous you can actually download the raw data from 23andMe.

And 23andMe has actually made an API so that if you want you can actually develop your own App for 23andMe and any person can download their raw data. Now most people will have no clue what to do with the raw data, but if they want to they can submit it to these other external Apps or use it themselves. The same thing should happen for healthcare, for the EMR.

The biggest complaint that I hear from patients is that they don't have an easy way to send their data to these sites, the burden is always on the patient.

So, if a person wants to contribute to PatientsLikeMe or to Sage Bionetworks, or Cancer Common, or a number of these other open patient communities where they're actually using the data for research purposes and for sharing with other patients the burden is always on the patient. So, for me what that meant, for getting my medical record I had to fill out all the paperwork and then I got about 20 CDs in the mail, I have to upload those all to my computer, you know, they're scanned PDFs and I have to transcribe all that data from these different sites.

So, if we had an API where it was under patient control you could say "yes, I approve sending this to PatientsLikeMe, I know it's not approved by the hospital, but this is my raw data and it's in a standardized set" and so PatientsLikeMe can accept it, right?

And we're already starting to see that happening right now. There's a number of companies that are developing API-like tools that scrape data through portals. So, for example, there is a company called Glimpse, right, and the whole point of Glimpse is it's an online platform where if you enter your patient portal user name and password, and they've developed these scraper tools for certain types of portals,

it will go and pull all of that information out and make it so that you can use it in this very easy way and reduce that burden. So, I hope that adds some clarity.

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

Yeah, thanks.

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

This is Adrian, let me take a different path through your question in four steps. Step number one is, I think the testimony we heard from Google and was mentioned by a number of people over and over is that the mechanisms to securely expose APIs to uncertified or unregulated, or open-source Apps are already in place for Google Docs and for all maybe 50 different APIs that Google exposes and they also talked about the procedures.

Number two, if we prioritize the use of the same API, FHIR API, for both providers and patients then we will be sure that these best practices come into play in a timely fashion and that was the key point of my testimony you might say.

Number three, unlike what...we don't want to do just what Steven just said, we need to have the ability to direct to third-parties, to direct the API to third-parties because that makes App development cost effective for that one and a half million Apps universe because they don't have to worry about provenance for example.

And number four, we have an example in hand right now with Blue Button on FHIR, here's a situation where there is a dataset, there's an established way to access the CMS claims dataset through a, you know, authorized portal and we have a federally supported effort to bring FHIR into...to update that to FHIR.

So, the federal health architecture is very conservative and very concerned, rightfully so about the privacy and security aspects if we can sort of jump from point number one, which is the Google testimony, to point number four, which is what do we pilot with Blue Button and FHIR in, you know, early middle 2016. I think we've closed this loop that Steven and I are both talking about.

Mark Savage, JD – Director of Health Information & Technology Policy & Programs – National Partnership for Women & Families

So, this is Mark, I just...I'm not an App developer but harkening back to your question, I think what we've tended to recommend is that we build for that diversity, design and build for that diversity so that different people can make the different choices if we are thinking about it ahead of time than the end-user gets to make that choice and the problem gets solved.

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

Leslie Kelly Hall?

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Great, thank you. I think we've got a couple of issues here and I'd just like to restate them. So you have the one issue where the App that's being registered to the patient, to the API at the provider's location you really cannot do that without the provider involved to grant permissions either the patient has

provided their identity to the provider, the provider has validated that and given them a logon to go in and register themselves to the portal or their API. And that does take the provider to be involved.

What we don't want to see happen is in that consent or registration of an App, to the wonderful guidance we received last week from OCR, on having the data once that App is registered, owned, controlled and at risk of the patient's use somehow conflated with the registration process in a way that makes the vendor providing the App, whether that App might be some third-party App or it might even be the tethered App or the Cerner App that the patient chooses to use to aggregate their data from all of those sites, we don't want that App to then have to be considered required to be under HIPAA because the vendor providing that App is actually in a different relationship, a BAA, with that covered entity. So, we want to make sure there's clear guidance on that relationship.

So the BAA in this case, maybe it's Cerner providing the data tethered EMR or the new App to the API, they have to be able to have a new relationship with the patient that says "hey, we're Cerner and you're about to use this great App, we'd really like you...we're going to gather more information with you and this information is between you and I and we may or may not share it with the provider based upon your preference, patient, and our relationship is now housed under the auspices of the FTC and not under the auspices of the HIPAA." So, I think there needs to be some understanding clarity if what I've just said is possibly true, not sure.

And then there's that other case where that App might be just the App that the patient has used and selected from a third-party that's never had a relationship with the covered entity. And then there's the Mint.com case which is, mentioned earlier, that I'm just doing my registration, my logon and my user ID to an App that's going to aggregate from all of my providers and now reuse it in a way that the provider has no knowledge of.

So, I think there are three possibilities that we need to have clarity on, the where HIPAA ends and a new commercial relationship begins with each one of those and I wonder if we could get some guidance from ONC about some of these legal nuances and other issues that were brought up earlier. Adrian's comment that, I think you said that it's illegal to have an App, an API different for a provider or a patient, I don't know that this is true. I'd like to find out about that...more about that as well. So, I don't expect...

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

Leslie, you just nailed my question as well about that particular requirement and everything that you said I completely echo as far as the three potential models of consumer control.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Because we don't want...

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

And it was...

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

We don't blocking to happen because the entity providing the App has a BAA relationship with the covered entity in another capacity.

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

Can I, I think it's true...

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

Hi, this is Linda Sanches from OCR.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Yes, great.

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

...

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

There have been many really interesting questions brought up today that touch on the HIPPA access requirements and the HIPAA security requirements and I'm not sure it would be helpful for me to address them all directly right now, but I do want to get a better sense in writing of some of these different scenarios you just mentioned and I think...I'd be happy to work with ONC to provide some response to clarify some of these questions.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

That would be wonderful, thank you.

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

Oh, you're very welcome.

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

I have...

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

Leslie, I can team with you if you want me to draft it up?

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

I'm sorry?

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Great.

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

I was volunteering to help Leslie draft the questions.

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

Okay, great.

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

You're name? I'm sorry, one more time?

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

Sure, I'm Linda Sanches and I'm with the Office for Civil Rights and we enforce the HIPAA rule so...

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

Okay. You work with Deven McGraw, yes?

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

Yes, I do.

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

Thank you.

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

Not...on a separate issue that was just brought up. I want to point out what...Eve Maler's testimony about UMA in that the technology that's behind HEART, which is User Managed Access, separates access control be it directly or through a business associate into two phases and this is very important.

Phase number one involves only the patient or the beneficiary, or the subject and the data holder, the HIPAA covered entity. And at phase number one we don't know who is going to come looking for that data, in other words who the third-party client will be, will it be a patient, will it be a licensed provider, will it be somebody that is certified in some way.

And then, you know, two weeks later with the UMA and HEART technology model, which is based on OAuth I should say just as FHIR is, when the third-party shows up at that HIPAA covered entity and says, please use this App and send me this particular's patients data, at that point the technology that was introduced in phase one by the patient in effect saying, you know, here is my surrogate, here is my lawyer for example that can speak for me as to which Apps are verified and which requesting parties are allowed to use these Apps, at that point these two things come together.

So, UMA provides this separation of the patient control component or the delegation ability of the patient from the actual transaction that then results in the data flowing directly from the HIPAA covered entity to the third-party that wants to use it. And this provides huge scalability and automation benefits because it then encompasses pretty much all of health information exchange including 42 CFR Part 2 and things like that. Once you separate these two things the whole system scales tremendously.

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

Adrian, this is Aaron, I was wondering if you could help clarify something for the committee and others about the way that UMA works. Would it be accurate in a shorthand way to say that it facilitates a consumer communicating their personal privacy preferences so that it can be implemented in an electronic exchange among entities?

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

Yes and it does so in a way that actually, as I just said, not only does it work for general clinical sort of TPO type access but it also scales all the way up to 42 CFR or sensitive data where the consumer preference is held to an even higher standard of privacy if you would. So it goes well beyond the opt in/opt out or the typical HIE issue and actually encompasses the full range of privacy requirements.

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

Where some of us might be willing to share our substance abuse history or whatnot which is difficult to do under their existing regimes.

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

Yes. And I want to also make a second point about the way UMA and HEART layers onto FHIR. We've had, you know, dozens of people talk about patient ID and matching with respect to it and it's very...you know my point is that when you use the same interface for both patients and providers or license practitioners the patient matching problem basically disappears. And the reason it disappears is because then you can do the kind of matching that we talked about when we used the finance analogy where, you know, people match themselves. But I want to make a comment about that.

We don't want to jump to the analogy of finance and credit bureaus in healthcare because credit is a privilege and because it's a privilege you have a choice to either play into the reputation scheme and benefit from having that reputation so that you get lower cost credit.

Healthcare is a right, at least, you know, from this privacy perspective, and that means that we don't have the right as a society to be coercive in how we track patients, just for instance because we could have iris scanners at every hospital and ambulance, and police cars for maybe \$100.00 bucks already, that doesn't give us the right to match and use these biometric tools coercively because it reduces the trust that patients, say mental health patients, have in the system and so it is not the same as what happens in the finance and credit sector when we apply these patient identity things.

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)

Thanks, I wanted to kind of come back to one thing Adrian that I think you asserted that I didn't exactly follow and I think Leslie kind of touched on just to see if you could maybe take another tackle at it with regard to having separate APIs for healthcare operations and docs and separate for consumers and why you feel...like to me that just makes sense there's a lot of APIs that I would develop from an operations perspective within the hospital that would only ever be exposed to, you know, people delivering care as a part of their job that would never be exposed to the consumer. Are you saying that there should be a subset that's common or what are you trying to say?

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

I'm trying to say that technically, at the technical level, we need to be absolutely the same. Now in certain cases we might layer policy-based constraints on for instance a physician opening up the API that they have internal, you know, when they're logged into their own EHR to a physician that happens to be in Saudi Arabia or whatever...

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

Yes.

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

Because that's the right thing to do. So, we are going to be able, we already know how to layer protections, policy-based protections and we've done this, you know, with faxes and US mail connection to health records for, you know, 100 years.

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

Yes.

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

So, but at the technical level when we talk about APIs and API-related policies we need to basically use this idea of the same FHIR API for both because then we're not taking away the safety valves of not just the patient things that Steven talked about...

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

Yeah.

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

But also the patient/physician relationship that also provides a major patient safety component.

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

I'm still struggling with it but we can talk about it more at some point. You're saying the same standards should underlie both technologies although the use cases may be different or no?

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

I'm saying exactly that.

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

Oh, okay, yes, got it, sorry, I was misunderstanding you then. There's no reason to have separate technology stacks to serve one use case versus the other.

Do you...does anyone from the consumer advocacy panel feel that there are aspects that we have...you know we've had just one day of testimony, I think this is the end of the testimony that we'll be hearing, is there anything that we haven't heard over the two days of testimony that we need to hear as we try to figure out practical recommendations that will make a difference?

Mark Savage, JD – Director of Health Information & Technology Policy & Programs – National Partnership for Women & Families

Aaron it's Mark, I have...

Steven Keating – Patient Advocate/Consumer – Doctoral Candidate, Mechanical Engineering, MIT Media Labs

I didn't hear the full first day so I'm not sure if this has been explored, but have you guys been talking to the major companies like EPIC and seeing how they will actually implement this?

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

Adoptability is something that we have touched on, you know, and...

Steven Keating – Patient Advocate/Consumer – Doctoral Candidate, Mechanical Engineering, MIT Media Labs

Okay.

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

I think KP actually touched a little bit on the notion of sort of a broker in the middle type concept that Tim McKay talked a bit about.

Steven Keating – Patient Advocate/Consumer – Doctoral Candidate, Mechanical Engineering, MIT Media Labs

Okay.

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

And is that what you're talking about adoptability and can the guys who actually are the resource owners or the data owners...what is their readiness to exchange. We did talk a little bit about that. Mark, was that you?

Mark Savage, JD – Director of Health Information & Technology Policy & Programs – National Partnership for Women & Families

Yeah it was and I was going to say the same thing that Steven said which is I haven't heard all the rest of the testimony so can't really answer your question...

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

Okay.

Mark Savage, JD – Director of Health Information & Technology Policy & Programs – National Partnership for Women & Families

And just wanted to let you know.

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

What is the most...what do you think is the most...if you had a trade-off to make, right, 80% of Americans having access to their data with some risks or 50% of them having access to their data with no risk which policy would you recommend to congress to society?

Deborah C. Peel, MD – Founder & Chair - Patient Privacy Rights Foundation

This is Deborah Peel, can you hear me? Yes, I'm with Patient Privacy Rights, I'm the Founder. The problem with these kind of questions are they completely ignore our very strong individual rights and that I think, having listened at least to part of this from the consumers is what you kept hearing, everyone who is not committed and not adjudicated incompetent is allowed to make their own decisions. And Americans and people around the world feel very strongly about making their own choices about risk. And so, you know, once again this is the kind of paternalism, what are we going to do that's better for everyone and it's not only insulting it's a violation of the law.

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

Deborah, I wasn't being paternalistic. I was asking a...

Deborah C. Peel, MD – Founder & Chair - Patient Privacy Rights Foundation

Well, when you talk about we have to choose between these two things, no we don't have to choose, we...

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

It was a hypothetical question I was trying to...

Deborah C. Peel, MD – Founder & Chair - Patient Privacy Rights Foundation

The consumer/the patients want...we want our choices ourselves...

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

Yes, agree.

Deborah C. Peel, MD – Founder & Chair - Patient Privacy Rights Foundation

And we need the information to make it. And we feel...

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

True.

Deborah C. Peel, MD – Founder & Chair - Patient Privacy Rights Foundation

Very strongly that...very frankly the law has always been, even in the paper age, that patients could get their entire records and that's certainly true of, you know, the clarifications to the HIPAA Privacy Rule, the datasets that we're supposed to be able to get from the EHRs include everything, financial data, raw data, every kind of data.

And, you know, so there are very good reasons for there to be one API, you know, as long as vendors and others control the data we'll never be able to...if we have to be regulated as if we can't handle things ourselves, you know, we're essentially cut off from the full view of our data and the full use it which is critical to be able to get not only second opinions but it's very clear that to be able to compare care between institutions the data holders don't want those kind of comparisons and the only people who do are in fact the patients.

And so it's a critical check and it's really the only way to get meaningful research is for us to be able to get all of our information the way that we always have been able to, you know, in the paper age it was laborious then but we had rights to it. And that really hasn't changed in fact, you know, we need that.

The other thing that we need to point out is really we...what's going on with ONC and HHS that we still do not have an ability to get a full accounting for disclosures from EHRs, you know, that's...it's now been, I don't know, what is it seven years since HITECH passed and we still have no accountability to transparency of the uses of our data and where it's disclosed by the data holders.

And so, you know, the fears about all the places will disclose our data are actually going to pale in comparison when we finally get data maps that show how far and how often, and frequently our health data is shared with third-parties, fourth-parties, fifth parties that we don't even know about.

And so the idea that, you know, people have to be protected from the disclosure or misuse of our data doesn't make sense given the fact that there a 100,000 health data suppliers in the country now that cover 780,000 live daily data feeds and we should be able to get all of that data from all of those people

that have our data. There are secret databases we don't even know about. And so the first step to any kind of equality really is an API that's the same. The same for everyone and I'll stop there.

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

This is Michelle...

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

Hey, Michelle...

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

I just wanted to note...

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

This is Meg...

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

For the record that Deborah Peel was invited to participate in the Q&A as she works with Adrian Gropper. So, I don't want there to be confusion about why Deborah was on the VIP line. Okay, so it doesn't look like we currently have any more...

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

Ah...

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

Questions from our Task Force members...

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

I have...

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

But let me just double check.

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

Yeah, I...can I just make one other point that I think needs to be made to the API Task Force? All of the testimony we've heard for the last two days presumes something that I don't think is going to be the case for very long and Steven made this quite clear and that is that right now we presume that patients do not own or have their own EHR technology, their own health record technology, as sort of the gold standard for that particular patient. We presume that, you know, every separate institution that serves the patient might have like nine or eleven different portals into separate EHRs and insurance, and pharmacy systems and whatnot, that this is the way it's going to be and we're going to have a network of networks of interoperability and consent management between all of these. And I want to point out that this is not where all of this ends up.

This ends up with the ability of individual patients whether working with a direct primary care physician or even without is able to have a standards-based access, you know, FHIR for example, a public API into a health record that is theirs, that is under their control and then it is up to the individual physicians and institutions as to how they want to synchronize with that particular patient's record.

And so I'm making this point because we don't want to stop with just this assumption that patients cannot have their own technology. And, you know, I don't know if Steven wants to sort of come in on this particular point but I think it is something that he and I would strongly suggest.

Steven Keating – Patient Advocate/Consumer – Doctoral Candidate, Mechanical Engineering, MIT Media Labs

Yeah, well, I mean, I completely agree and in terms of the taking risks I completely support what was just previously said and I think it's interesting to think about, you know, the compassionate care clause as well where if patients understand the liabilities they're taking they're able to go get past the FDA there should be the same thing on the data side.

It's so crazy right now that I don't have access to my own tumor genome that's...you know it's insane and the reason I don't, even though my doctors and researchers want me to have access, is because it was...there's a potential CLIA conflict and so if the API has these standard sets which allow access to raw data, right, then a lot of these issues can be resolved and patients can then actually move forward making their own decisions and taking their livelihood into their hands.

You see that with Facebook, you see it with Twitter, any time someone puts a Tweet out and puts a picture of their house, yeah, they're taking a liability that someone can know they are, you know, not at home right then and they can break into their house, right? You put up a picture of you on Facebook drinking a beer and maybe your employer is not going to hire you, right?

So, there's always inherent liabilities and we need to have the same thing and allow patients to make their own decisions taking those liabilities into their own account. We can't have...right now the doctor is God and instead we need to have the doctor as a guide, right. The patient needs to be informed to make their decisions and having access to data through an API can enable that.

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

Steven, if you...

Deborah C. Peel, MD – Founder & Chair - Patient Privacy Rights Foundation

Steven, this is Deborah, it's not doctors that are blocking this it's the institutions, it's the data holders because our...

Steven Keating – Patient Advocate/Consumer – Doctoral Candidate, Mechanical Engineering, MIT Media Labs

Yes, absolutely.

Deborah C. Peel, MD – Founder & Chair - Patient Privacy Rights Foundation

Data is valuable...

Steven Keating – Patient Advocate/Consumer – Doctoral Candidate, Mechanical Engineering, MIT Media Labs

Absolutely, absolutely.

Deborah C. Peel, MD – Founder & Chair - Patient Privacy Rights Foundation

And they've view it as their asset not ours. So...

Steven Keating – Patient Advocate/Consumer – Doctoral Candidate, Mechanical Engineering, MIT Media Labs

Yeah.

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

If you end up working for somebody who doesn't want you to be drinking of beer you're better off losing your job. I thank you guys very much and I actually, you know, really appreciate your input to this and I'm sure anyone else on the call does.

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

Okay, so one final check from the Task Force to see if there are any more questions? Okay, hearing none, thank you to all of our panelists today we greatly appreciate you taking the time. I am now going to turn it over to Meg and Josh to make a few concluding remarks.

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

Well, thanks very much Michelle and thank you to all of our panelists it's really been a lot of great testimony that we've heard today covering a wide range of perspectives and topics and quite a lot of depth and I really appreciate the level of depth that we were able to get into talking through a number of these issues.

What I think we'll do is to offer pretty quick summaries just from Meg and me of the panels that we heard and then open up to public questions. So, I think the way that we've tried to divide it that Meg will summarize the first panel we heard today and then I'll summarize the second two panels that we heard.

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

Hi, thanks, Josh and again, thanks to everyone. Panel 3 earlier this morning just sounds so far away. So, here's some of the main themes that I took note of.

We heard about the balance between implementing a Good Housekeeping Seal and allowing open access to a large number of Apps based on consumer choice but that there may be additional standards and discussions around governance that would be helpful. That this "feel like concept" we heard thoughts on whether this could be a standards body or regulation, there are certainly pros and cons to both.

We heard from some providers who generally believe that they have an obligation to protect their systems but in the spirit of open and seamless access believe protections do need to be in place that are well understood across the industry as best practices.

We were reminded to remember small provider communities and their ability to access technical resources to support large scaled data movements as well as resources to support compliance activities.

There is a thought that as we move forward as an industry to standardize that information and standardize the technology, and standardize the legal and compliance components that this burden will not be any greater based on the provider's side, but some of us...somewhat of a thought that there might be a stepping up toward that we could potentially take into consideration.

We heard some discussion on the importance and challenges of identity proofing and patient matching. We were reminded that there are current processes out there that support these activities now, especially those related to portal access, so we could be mindful of alignment and leveraging those.

And we discussed data provenance and the importance to track and indicate where data comes from. So, those are my thoughts around Panel three.

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

Thanks, Meg and I'll just give a quick summary of some of the notes that I took in the fourth and the fifth panels.

So, in the fourth panel, you know, we heard the value of standards-based interoperability and the need from the developer perspective for standards that are very concrete and that provide a lot of detail and don't leave a lot of things optional.

And we had a discussion about whether authorization and data standards can be separated or whether these really come hand-in-hand.

We heard about the importance of vendor organizations and provider organizations working together to create a secure environment for data sharing and that there are responsibilities on both sides.

And we heard about the importance of governance for applications as one of the biggest bottlenecks to actually deploying new tools and services within the hospital environment. The focus there was mostly on provider-facing Apps for that conversation but there's a similar set of concerns to be sure for patient-facing applications.

And we heard the perspective that when we begin opening up data through these APIs, whether it's for clinician or for patients, there will be errors and yet there's still value in doing it even though we know that there will be mistakes along the way. We still need some way to move forward and that an important part of the way that we address this entire set of problems is how do we fix these errors after they've happened, how do we plan for that in advance.

And then briefly, from this most recent panel, you know, we heard that healthcare consumers are a very diverse group and some are worried about sharing data with a dangerous App or a rogue App and some people want to write their own Apps and mash up their data and 3D print their brain tumors.

And we heard about the importance of distinguishing, especially in the research sphere, between what you might consider raw data for which full access should really be provided versus analysis for which, you know, there might be more controls over the timing and the degree to which an analysis of those data are shared with research participants.

We heard about where the analogy between healthcare and finance that we so often hear can break down and this was Adrian Gropper who said that credit is a privilege and you have a choice about whether you want to pay into the financial reputation schemes or not but healthcare is a right and maybe that actually leads to different conclusions about the kinds of data access that we want to ensure. So with that, I think I'll turn back over to Michelle for public comment.

Public Comment

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

Thank you Meg and Josh. Okay, operator, can you please open the lines?

Lonnie Moore – Meetings Coordinator – Altarum Institute

If you are listening via your computer speakers you may dial 1-877-705-6006 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

And also as mentioned earlier there is an e-mail address on the screen if you would like to send some additional comments or some public comment for us to share that e-mail address is [faca-onc@altarum.org](mailto:fac-onc@altarum.org) and while we wait for questions there were a few comments put into the comment box of the chat and we'll share those with the members of the Task Force following today's meeting.

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

Michelle, this is Meg, just a quick question, for those who are submitting comments outside of this process to that e-mail is there deadline by which you'd like them to adhere?

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

The sooner the better so that we can follow up on recommendations as an outcome of the hearing. It probably would be most helpful to have before the next meeting of this Task Force, if I had the data at my fingertips it would be easier, but I don't what it is right now, let me look that up. So, the next meeting is February 9th so I would say the deadline should be February 8th so that we can have time to look at things beforehand.

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

Great, thank you.

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

Thanks, Meg. Okay, it looks like we nobody lined up to make a public comment. So, again, thank you everyone for participating in both hearings both Tuesday and Thursday, they were long meetings but very beneficial and we greatly appreciate all of our volunteers taking the time out of your busy schedule to share your insights with us. So with that, thank you to everyone and enjoy the rest of your day.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Thanks, Michelle.

Mark Savage, JD – Director of Health Information & Technology Policy & Programs – National Partnership for Women & Families

Thank you.

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

Thank you.

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

Thanks, everyone.

Steven Keating – Patient Advocate/Consumer – Doctoral Candidate, Mechanical Engineering, MIT Media Labs

Thanks, take care.

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

Thank you.

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

Thank you.

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

Thanks.

Public Comment Received During the Meeting

1. Joseph Arnold: I would like to have the panel address what role to they see API Gateways in providing security and standardization?
2. Ann Racuya-Robbins: Can we be reminded of the scope and meaning of privacy? Are you talking about a narrowly construed PII? In the UMA context?
3. Nick Saunders: didn't clinics ask you to pay for those records though?
4. 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	01/28/16	01/26/16	01/12/16	12/04/15	11/30/15
Aaron Miri	X	X	X	X	X
Aaron Seib	X	X		X	X
David Yakimischak	X	X	X	X	X

Drew Schiller	X	X	X	X	X
Ivor Horn		X	X	X	X
Josh C. Mandel	X	X	X	X	X
Leslie Kelly Hall	X	X	X	X	X
Linda Sanches	X	X	X		X
Meg Marshall	X	X	X	X	X
Rajiv B. Kumar	X	X	X		
Richard Loomis	X	X	X	X	X
Robert Jarrin			X	X	X
Rose-Marie Nsahlai	X	X	X	X	X