



**HIT Policy Committee
HIT Standards Committee
Joint Meeting
Application Programming Interface Security Task Force
Transcript
November 30, 2015**

Presentation

Operator

All lines are bridged.

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

Thank you, good morning everyone, this is Michelle Consolazio with the Office of the National Coordinator. This is the first meeting of the API Task Force under the Health IT Standards Committee. This is a public call and there will be time for public comment at the end of today's call. As a reminder, please state your name before speaking as this meeting is being transcribed and recorded. I'll now take roll. Meg Marshall?

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

Here.

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

Hi, Meg. Josh Mandel?

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

Hi.

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

I'm here.

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

Hi, Josh. Aaron Miri?

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

I'm here.

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

Hi, Aaron and Aaron Seib?

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

Present.

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

Hi, Aaron. David Yakimischak? Drew Schiller?

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

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.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Hi.

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

Linda Sanches?

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

Hi, this is Linda.

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

Hi, Linda. Rajiv Kumar?

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

Hi, this is Rajiv, good morning.

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

Good morning, Rajiv. Richard Loomis? Robert Jarrin?

Robert Jarrin, JD – Senior Director, Government Affairs – Qualcomm Incorporated
Hi, Michelle.

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

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology
Good morning and Jeremy Maxwell?

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology
Hi, I'm here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology
Hi, Jeremy, anyone else from ONC on the line?

Richard Loomis, MD, CPC – Senior Medical Director & Informatics Physician – Practice Fusion
Hi, this is Richard Loomis just joining.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology
Hi, Richard, thank you. Okay with that I'm going to turn it over to Meg and Josh.

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

So, thank you, Michelle. Thanks everyone for joining this inaugural call of our Workgroup on API Security Task Force. I think that we are going to go through the agenda but one item I did not see on the agenda was, oh, never mind I just can't read, some member introductions. So, I want to start with a quick introduction of myself then I'll pass it over to my Co-Chair Meg Marshall and then we'll go around for everyone who is on the call just so we know who is involved in the group.

So, I'm Josh Mandel, I'm on the Research Faculty at Harvard Medical School. I've been working over the last five years or so on a Project called SMART Health IT which has been all about putting up EHRs and personal health records for applications that can plug into those systems and help users make sense of the data in them. So, I've been really focused on the subject of APIs in my work over the last five years or so.

And for me, the areas that have been of the most interest have been number one, clinical content which is an area where healthcare APIs really bring their own unique considerations to the table and then number two has been security considerations of these APIs and making sure that we can provide access to data in a way that's secure but also consistent from system to system. That's just a quick introduction and let me pass it over to Meg.

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

Hi, great, thanks. Thanks, Josh. Thanks, Michelle. Good morning. My name is Meg Marshall I am Director of Health Policy at Cerner. Cerner is a Health IT company whose technology offerings include electronic health records and consumer-facing functions.

I personally have 20 years' experience in health IT with a level of expertise in legal and policy issues including privacy and security. I also have active roles in various industry organizations including the Electronic Health Records Association, HIMSS and eHealth Initiative.

And I just wanted to say I'm very excited to be working with this group of subject matter experts and that I'm supported by such wonderful talent at the ONC. I think this is a very important discussion. It is very near and dear to me and again I'm excited to be a part of it. So, thanks.

What may make sense, I don't know, Josh or Michelle, the easiest way to approach the member introductions is that alphabetically or...

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

I would just go down the list of what is on the screen.

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

Okay.

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

So, Leslie Kelly Hall would be next.

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

Hi, thanks, I'm Leslie Kelly Hall, I'm with Healthwise a non-profit committed to helping people make better health decisions, a 40-year-old non-profit in this space. I'm a former chief information officer turned consumer advocate after giving access to 700,000 people their medical records across seven healthcare organizations in Idaho and very committed to making sure that people have access and are able to use information with the best possible education behind them to better understand their health, and excited to be here. I'm also part of, I think that I mentioned, the Standards Committee and DirectTrust, and many other organizations committed to interoperability. Thank you.

Robert Jarrin, JD – Senior Director, Government Affairs – Qualcomm Incorporated

Hi, there I guess I'm next it's Robert Jarrin with Qualcomm Incorporated. I help direct Qualcomm's public policy agenda in Washington, DC on wireless health and life sciences. I also represent our medical device subsidiary Qualcomm Life and a number of other entities which we've acquired over the last couple of years. My focus is typically wireless health but that obviously includes the broader ecosystem of health information technologies.

I've been very lucky and fortunate to have worked in the past on several other FACAs including FDASIA most recently with Meg, actually, so, hey, Meg. And I'm really looking forward to this FACA Workgroup in particular or I guess we're calling it a Task Force because APIs is something that is of most importance to many of the 200+ organizations that work with Qualcomm Life. So, with that, thank you.

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

Rajiv?

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

Hi, this is Rajiv Kumar, I'm a Pediatric Endocrinologist at Stanford's Children's Hospital and Medical Director of Clinical Informatics, and I've been charged with using the medical and home wearables to absorb patient generated health data into our EHR and then to strive for interoperability among other EHRs to learn about chronic disease and so we've done this recently with using continuous glucose monitors that passively absorb data through an Apple phone or iPod into EPIC through the My Chart patient portal App and have just had a lot of up's and down's trying to get the workflow going and realize that using data viewers and APIs definitely lower the threshold barrier for providers to adopt and so I really got interested in this space and thanks for inviting me on the Task Force.

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

Richard Loomis?

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

Hi, Richard Loomis, I am the Chief Medical Officer at Practice Fusion. I oversee both health informatics and medical affairs in my role. Practice Fusion is a cloud-based EHR vendor and APIs are of critical importance to our ability to deliver interoperability to our users and ultimately their patients. My clinical background has been anesthesiology and I have advanced training in medical informatics as well. Looking forward to working with everyone on the Task Force.

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

Good morning everybody this is Aaron Miri, I am the Chief Information Officer for Walnut Hill Medical Center here in Dallas, Texas. Prior to this life I was the Chief Technology Officer for Children's Medical Center of Dallas. I also serve as the Chair of the Public Policy Committee for HIMSS. I served on the Policy Committee of CHIME and this is my second FACA, I was on the Transport and Security Task Force as well. So, look forward to working with you all on this. I personally believe this is a crucial topic to the industry and as we move the ball forward I look forward to the progress we're going to make.

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

Hi, this is Drew Schiller, I'm the Co-Founder and Chief Technology Officer at Validic. Validic is the industry's leading platform for connecting patient generated health data from digital health Apps, wearables, in-home medical devices into the healthcare system. So, we work with EHRs, hospital systems, large HIT vendors, pop management companies, anyone really who is looking to connect data from outside the four walls, that is generated outside of the four walls of the hospital, and bring it back in.

So, APIs are really important to us, you know, we connect with well over 200 devices and we were deployed in 47 countries 260 million lives and so this is a really important topic for us as we continue to move forward on the patient generated health data path and interoperability.

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

Good morning my name is Aaron Seib, I'm the CEO of NATE also known as the National Association for Trusted Exchange. I've had the pleasure of serving on several FACAs in the past including FACAs related to governance and security and privacy. I really am humbled to participate with this esteemed group. I think that we're working on some things that will make historical changes for the benefit of consumers and providers alike.

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

Good morning this is David Yakimischak from Surescripts just checking to see can you hear me?

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

We can hear you.

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

Okay, great, hi, everybody. Sorry, about that I think we need an API for our computer microphones because I was trying to use the IT mic and that wasn't working. So, hi, everybody I'm a Senior Vice President in Information Systems at Surescripts and previously for nine years had roles as Chief Technology Officer, Head of Clinical Quality as well as General Management.

And Surescripts operates the National ePrescribing Network over 800,000 doctors, 65,000 pharmacies, 1.5 billion prescriptions a year, about 2/3 of the prescriptions in the country. Obviously, on both a personal, professional and national basis think that APIs are key to interoperability. It is something that I'm really looking forward to participating in and thank you very much for having me.

Ivor Horn, MD, MPH – Medical Director, Center for Health Equity – Seattle Children's Hospital

Hi, this is Ivor Horn, I'm the Medical Director of the Center for Diversity in Health Equity at Seattle Children's and Professor of Pediatrics at the University of Washington School of Medicine. I am honored to be on this Task Force with this very prestigious group of folks. I am a pediatrician and a researcher interested in the intersection of health communication and health disparities particularly as it relates to use of technology and how we can use that to improve health outcomes for underserved populations.

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

Thanks, Ivor. Linda Sanches?

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

Sure, hi, this is Linda. I'm with the Office for Civil Rights which of course provides guidance for compliance with the HIPAA Privacy and Security Rule. The focus on my work the last two years is on health information technology and privacy/policy related to HIPAA Rule protections. I've worked in health information privacy/policy and HIPAA compliance enforcement for about 17 years and I'm very excited to be part of this group and looking at how these more recent technologies can be used to help consumers. Thank you.

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

Jeremy and Rose-Marie do you want to introduce yourselves?

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

Sure, you go ahead Rose-Marie.

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

Sure, this is Rose-Marie Nsahlai, I'm with the Office of the Chief Privacy Officer at ONC. I'm an IT Security Specialist. Prior to that I worked in IT at a consumer product company and did HIM work at hospital systems and EHR implementation. I'm really thrilled to be part of ONC and working with this group. Thank you.

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

My name is Jeremy Maxwell, I will be supporting Rose-Marie as the staff support for this Workgroup. I work with her in the Office of the Chief Privacy Officer here at ONC. I am a software engineer by training. Prior to coming to ONC I worked for five years at Allscripts as their security architect heading up their privacy, security and compliance team.

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

We also have supporting the group from ONC Lucia Savage who is our Chief Privacy Officer and Maya Uppaluru who I think is on the public line. So, you'll probably hear their voices at some point in the future so be on the lookout for them. Okay, with that thank you all for agreeing to be a part of this group. We are so fortunate to have such a diverse mix of folks and we really appreciate you agreeing to participate. I'm going to turn it back to Josh and Meg.

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

All right, thanks very much Michelle and thanks everyone for your introductions. I'm really excited about this group, about everyone who is able to join us and what I'd like to do is dig right into the charge for the Task Force. I think we have one background slide and then a few bullet points worth of what we're actually here for.

All right, so on the background side, just so everybody is up-to-speed on the acronym, API is an Application Programming Interface and the goal here is this is some technology that lets one piece of software talk to another piece of software in a programmatic way. So, it's all about the automated functionality by which you can control how the software works.

And APIs have been invoked, in particular, in the 2015 Certification Rule. So, ONC has a certification criterion that describes an API that supports a patient's access to health data so there is something called view and download and transmit, and then a set of APIs that access structured health data.

Over the course of the proposed rule and the comment period for the proposed rule there was, back from some of the Federal Advisory Committees, as well as from the public and the comment period, where members expressed concerns about privacy and compliance of these APIs, and so today we're launching this API Task Force to help address some of these concerns, specifically to be able to lay them out, understand them and then make recommendations about how to move forward.

So, onto slide four, this is our Task Force charge and the questions that we've been charged with answering. So, the first two bullet points here are almost identical. I'll just point out the difference for you start, the first one is about security and the second one is about privacy.

So, first bullet is to identify perceived security concerns and real security risks that are barriers to the widespread adoption of open APIs in healthcare. And then in particular for the risks that we identify as being real to figure out which of those risks aren't currently planned to be addressed in the Interoperability Roadmap from ONC. So, for example something things like identity proofing and authentication and these aren't unique challenges for APIs but these are important components of the ecosystem. So, that's the security and security risk point.

And then moving onto the privacy and privacy risks we have a charge of identifying perceived privacy concerns and real privacy risks that again are barriers to the widespread adoption of open APIs in healthcare. And for risks that are identified as real figure out which of those aren't already planned to be addressed in the Interoperability Roadmap and the example here is harmonizing state law or the fact that HIPAA is often misunderstood or misapplied.

And then finally, we have a charge of identifying priority recommendations for ONC that will help enable consumers to leverage API technology to access patient data and at the same time ensure that the appropriate levels of privacy and security are protected. So, the goal here, in this third charge point, is really that the specific focus is on consumer access of these technologies.

So, on the following slide we have a list of related issues which we've attempted to define as out of scope and I expect that these are issues that we'll continue to bump up against in the course of our discussions and in the course of our planning and so we'll do as much as we can to explicitly identify them when they come up and put them to the side, but I suspect there will be areas where these simply interact with the privacy and security concerns and to the extent that they do then we'll take them up, but we're leaving out of scope things about terms of use, who can use the APIs, the licensing requirements about how API access is licensed, policies and the formulation of those policies to access these APIs or how, or under what condition, the fee structures or charges that will be needed to provide this API access or anything about certification authorities, who says who is allowed to access which APIs and standardization.

So, we're not charged with formulating standards by which these APIs work or the security standards, we're really focused on these high-level questions of, how can we provide things that are secure and what are the concerns about security and privacy. So, that's the goal at least is that these set of issues is out of scope. So, before we move onto the proposed work plan are there high-level questions about the scope of this charge and the things that we've left out of scope? I'll just open up for comment here.

All right I'll assume that I've at least spoken clearly enough that some of these ideas have gone...let me dig into those proposed work plan.

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

Josh, this is Aaron, I would agree.

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

That comment was an “okay to move forward?”

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

Yes, move forward, I think you were very succinct and were prepared.

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

Okay, good. So, on the work plan we sent out a list of meetings that will span from this opening call today through an April 19, 2016 meeting where we present a set of final recommendations to the Health IT Standards Committee and Policy Committee.

And in order to get us there we have a path that will take us through a set of virtual hearings where we will first identify a set of questions that we want to solicit feedback and concerns from the community about we’ll identify which presenters we want to hear from and then in January we’ll have these two hearing sessions which will be a total of...what we’re looking at is 10 hours of testimony that we’ll collect.

And then our charge in February and March will be to synthesize what we learned from those hearings into a set of recommendations that will be presented in draft form in the middle of March and then a final form in the middle of April. So, this is the arc of our next five months of work together and I’m really looking forward to digging in as we start to work through these issues.

So, let me...so first of all are there questions about the proposed work plan or the table that we’ve laid out here?

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

Yeah, hi, this is David Yakimischak from Surescripts, given that this does extend fairly well into next year have you considered maybe making an optional face-to-face for one of these Task Force calls that way if people want to have a chance to come together and actually meet each other maybe in the DC area out in March or April of next year that we could do so?

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

That’s a great question...

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

Ah...

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

It is something that had come up. Michelle, please?

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

Yeah, as you can imagine flying people in is a lot more costly than doing things virtually. So, because of the short-term nature of this group we’ve decided to make everything virtual at this point. It is

something that we could talk about but based upon our current budget I think we'll need to do things virtually for the moment.

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

Would it be out of bounds to have something like an optional show up in person date where people who can travel show up in person but we do everything virtually in terms of the telecommunication?

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

I mean that's certainly something we could talk about. We could think about doing something around the committee meetings where other people will already be in town.

David Yakimischak – Senior Vice President & Chief Quality Officer – Surescripts
Right.

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

It is something that we can brainstorm around.

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

Cool, so let's talk through that as we get closer to planning, you know, we're probably looking at early 2016 where that would become relevant and that's an interesting concept.

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

So, yeah, this is Aaron, I agree, I think that would be great and, you know, even the earlier the better for us all to, you know, make a facial...face-to-face meeting on a voluntary basis.

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

Great, and other questions or comments on the proposed work plan? All right, well, let me dig into a little bit of the background about how we got here today. I'll talk through in a little more detail about what some specific concerns are and in more detail about where APIs are invoked today and then I'll turn it over to Meg for a summary of some of the HIT Policy Committee concerns that have been raised in previous Workgroups.

So, first of all a little bit of background on APIs, you know, as a technology APIs can be subject to privacy and security vulnerabilities, we've seen this in the consumer world certainly, but APIs are also fundamental to the way that large scale data interoperability can grow and progress.

And we see that APIs are widely used outside of healthcare in other industries like finance and government and even consumer data access. And we see in those domains that privacy and security concerns are very similar structurally to the kinds of concerns that we have in healthcare.

So, part of what we need to do is to try to understand and address whether there are issues here about privacy and security that are unique when it comes to APIs for the interoperability of healthcare data and if they're unique in healthcare how would we prioritize and address them. And if they're not unique where can we learn from and adopt decisions that are made in other industries. So, our goal here is to get the Task Force to help us in that process.

So, some background, why are we here today talking about APIs? So, first of all, there is HIPAA and the Omnibus Rule of 2013 and I'm going to read to you off these slides so I apologize in advance for doing this but the background that we're working with here is patients right to access and in particular we have a provision that when a covered entity uses or maintains an electronic health record with respect to protected health information of an individual that individual shall have a right to obtain from the covered entity a copy of such information in an electronic form and the individual may direct the covered entity to transmit such copies directly to the individual's designee provided that any such choice is clear, conspicuous and specific. And then later on we have a strengthening of this rule with respect to covered entities that use or maintain an electronic health record.

So, this is part of the fundamental background on which we're working is an environment in which individuals have a right to access their data, they have a right to access their data in an electronic format and at the level of rights, they have the right to have a copy of the data provided to whoever it is that we designate as long as we can clearly expressed all of that in a way that the healthcare provider or organization, the covered entity can understand.

So, that's the backdrop and then more near-term backdrop thinking about the Meaningful Use Stage 3 and the 2015 certification criteria. First looking at what's in the CMS Meaningful Use Stage 3 Final Rule. There are a few places where patient access and APIs are explicitly invoked. So, there are two objectives in the rule, objective five and objective six which are about patient's electronic access to health information and the coordination of care through patient engagement.

And then CMS makes it clear that there are four basic actions, four activities that a patient or a patient's representative needs to be able to take with respect to these data. So, patients and other representatives need to be able to view their health information, to download it, to transmit to a third-party and to access the same information through an API. And so whereas in the previous round of Meaningful Use we just had view, download and transmit here we have now an explicit requirement of API access as well.

And then CMS believes these actions might be supported by a wide range of system solutions and these system solutions are going to overlap in terms of the software functionality that they provide in terms of how they help a patient do each of these things and these systems are also going to provide access for clinicians to exchange data directly with other healthcare providers in addition to patient access. So, there are a number of areas where the same kind of data and potentially the same APIs might be used, different use cases if you will.

And then CMS proposed that patient electronic access to allow providers to enable API functionality be done in accordance with ONC requirements. So, here we have a link between what it takes for a provider to be able to attest to Meaningful Use and then a set of certification criteria and so CMS says in order to be eligible for Meaningful Use you need to do these things and you need to do them with a certified EHR technology under the hood.

So, moving onto the next slide we have what are the requirements for that certified EHR technology under the hood and this is where ONC's certification criteria play a role and in the 2015 certification criteria we have an explicit criterion something that each EHR system would be able to be certified for that is to demonstrate that it can provide API access to something called a common clinical dataset via an API.

And there is actually three sort of separate criteria when it comes down to how a system actually certifies against this requirement and these criteria break down into allowing an application to select a patient, allowing an application to request data in a particular category like for example medications for lab results or immunizations and then finally, allowing an application to request access to all data about a particular patient. So, those are the three certification criteria when we boil it down...criteria when we boil it down to what does an EHR need to actually show.

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

Josh?

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

So, is there a question or comment? Please?

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

Josh, it's Aaron, I have a question about the definition of the common clinical dataset and not to get too technical or anything, but data goes through different states, right? Does the common clinical dataset define what states that data should be in before the API supplies it to a request?

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

Can you give an example of what you mean by state just so I know we're talking about the same thing?

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

Sure, so if I'm a provider working in a hospital and I create some EMR, you know, I have an encounter and I create some data that data goes through several quality assurance steps before it is considered final and ready to bill, also before it's really displayable via the patient portal, as an example.

So, it goes from a state of, you know, created, you know, just for simplification it's created, in a state of created, QC approved and then a status of ready to display. Does any of that concept come into play in the definition of the common clinical dataset?

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

So, the short answer from me Aaron is "I don't know" and there maybe someone else on the line who is better informed to answer that question.

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

I wasn't sure either that's why I asked, thank you.

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

Yeah, hey, this is Jeremy Maxwell from ONC. So, that is a little too granular for what we've defined in the regulation. So, you can find the definition of the common clinical dataset in the 2015 edition Certification Rule and I can send it to Michelle and she can distribute it to the group. I'll just extract the pages from the rule that it's actually in.

But defined in the rule, the common clinical dataset is things like, you know, demographical data like patient name, sex, date-of-birth, race, ethnicity, etcetera and then as well as the clinician information like medications, problems, allergies, lab tests, vital signs.

So, we don't get into the detailed, you know, data states as you describe them. We talk about it more at the categorical level I guess would be a way to describe it. But we can distribute that to the group.

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

I just raise that as one of the areas where there seems to be, you know, some consternation and fear on the side of, you know, different stakeholders in the market. If we could make it clear that it is only the final state that might relieve some of the concerns I think.

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

Hey, Aaron, this is Aaron Miri, I think the best way, as somebody once told me, is think of it like a clinician and what data is actually relevant to you as a clinician if you wanted to do an assessment on your patient.

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

Yes.

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

So, I totally get where you're coming from a technical perspective but the way the ONC tackled it, which I think the market, at least from all the CIOs perspectives was, what data do I need to be relevant...what data is going to be relevant to the clinician and to the data to make an accurate assessment. So, try to think of it that way when you look at these types of things.

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

That's really good, a message that we can share with people, I like that. A clinician is not going to be interested in what the state is between creation and QC but what that final state is right?

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

Yes.

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

Thanks, Aaron, good name too.

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

Ditto.

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

So, I mean, I think this is...Aaron's question there is a perfect example of an area where, you know, as many people read these rules and begin implementing the data access inside of real systems we're going to have hundreds of very specific questions about what should be included, what shouldn't be included and at the level of the certification criteria that we don't always have direct answers, at the level of the actual testing procedures we may have more direct answers but a lot of this may come down in the end to clinical judgement.

All that said, I'll also highlight this as an issue that is critically important, we need structured advice but it's out of scope in terms of our charge here and I'll emphasize that point again as we move forward, but, you know, our goal here is to focus again on security and privacy concerns rather than on how well defined these APIs are but it is a perfect question where Aaron asked it which is about background what are the requirements, what are we expecting these systems to do.

So, I don't mean to say Aaron that you shouldn't have asked that question it's a great question I'm glad you asked it. I think as we dig in there maybe areas where we'll say "yes that's important, no we don't know." But we're not going to deal with it right now.

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

I'm...

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

Hi, this is David...

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

Go ahead.

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

Yeah, this is David Yakimischak from Surescripts. The focus of this seems to be primarily on patient access but there is mention in a couple of places of sort of a spillover into provider to provider. So, are we clear that we have to address both flavors of API or are we looking strictly at the needs for consumer access as mandated through the regulations?

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

This is an important question about our charge and the way that I've read it we've been instructed to focus on consumer-facing use cases even though we know that some access to privacy and security that applies to consumer use cases will also apply elsewhere but if anyone from the ONC group wants to clarify that definition or Meg if you want to weigh in there I'd be very happy to have somebody tweak or correct my perception.

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

Josh, this is Rose-Marie from ONC, you are correct we will be addressing both flavors as mentioned.

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

So, I'm sorry, could someone repeat what the scope includes both the provider use case of the API and the consumer use case of the API?

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

That is correct.

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

Yeah...okay, because I had said we were focused on patients and then Rose-Marie's agreement actually said, no we're focused on both.

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

Right. Can we block and tackle, start on consumer and then expand to provider as a work plan? I'm sorry, I probably should keep my mouth shut, but that came to mind. That might be one way to simplify the problem and solve it for one of the two and then look at expanding it for the second.

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

Yeah, I mean, from the perspective...from my perspective in terms of scoping our work I think that makes a lot of sense. I mean, I think we'll probably have the discretion to figure out the order in which we will approach and if we want to do kind of a depth first we'll try to treat both at the same time. So, Aaron I think that makes a lot of sense.

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

Yeah, like make a statement that we're focused on the consumer with the intent of, you know, being future ready to expand to providers as, you know, we've got months here but let's start with just consumers.

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

So, this is Meg and Rose-Marie I'm not sure, maybe this might be worth you chatting a little bit more about, but back on slide four the Task Force charge in question the first two bullets that are security and privacy related those are fairly generic, those are open APIs in healthcare that I think that's to Rose-Marie's point where we do both the consumer and the provider, but the third bullet point specifically is consumer and that's priority recommendations that will enable consumers to leverage API technology to access patient data.

So, it does seem like we're heavily weighted toward the consumer aspect and I agree that this makes sense to tackle first but from...and I know that we've kind of wordsmith'd a little bit back and forth on that charge, the first two bullets, but that does allow us to talk a little bit about privacy and security as it also relates to the view, transmit, download APIs from provider to provider.

So, I think that's a good thing in that we're not too narrowly focused that we can talk about the ramifications of both.

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

That makes sense.

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

Good, so let me...I think I've got one more slide in terms of the regulatory background and then just a little bit about some of the public comments that have been received to date. So the last slide on the regulatory side is the one labeled 12 here, which is one more point on the certification process.

And so, in addition to being able to do patient selection and requesting data by category, and requesting all the data about a patient a system that is going to be certified needs to be able to provide authentication, access control and authorization and needs to support what is called trusted connection, it needs to do auditing of the actions that occur on healthcare data and it needs to support auditable events and tamper resistance.

So, there is a bit of security specific language that's sprinkled throughout these requirements with direct impact on the way a system is certified to be able to do these kinds of functional things on behalf of a patient. So, you've got the functions that it needs to support and then under the hood it needs to do them in a secure way. So, that's just a little bit of the language from the certification rule as they're written for 2015.

So, that's the regulation sort of background and I'll take you through just a couple of slides of comments, summarizing comments that were made when this was a proposed rule and so there were 51 public comments that were specific to the API certification criteria and they came from a variety of stakeholders including individual companies building tools that would like to use the data from EHR vendors building tools that would have to expose the data from provider organizations and from others.

So, 25 of these comments, the majority of them, focused specifically on a concern that the API certification criteria didn't specify a standard API, it really just specified functionality like let a patient download data by text or let a patient access all of their data through an API. It didn't specify which API or how the API should work or whether there was a standard API that needed to be used.

And so half of the comments were really focused on that point to say, without specifying the standard API we're not going to achieve interoperability and I'll just make a personal comment that from my perspective it's an incredibly important point, I honestly don't know the extent to which we can really get useful interoperations of systems without actually standardizing an API but it's not our charge here to worry about that point.

Our goal is to take for granted the fact that these are early days, that today we have a functional specification saying what it is a patient needs to be able to do and not a lot of detail about how, not a lot of detail about, you know, what are the particular URL paths and how are the parameters encoded and what are the file formats that are recurrent. So, it may very well be an issue but it's not our issue here today.

But that leaves us with a number of comments that do relate to the areas of our charge specifically to privacy and security issues in these APIs. We got 19 comments in that bucket of which about half, 10 of those comments, came from EHR vendors. We had a couple from healthcare provider organizations, two independent commenters, two professional associations making comments, one comment from an academic institution, one from an advocacy group and then one from a consulting firm. This gives you sort of a breakdown of the 20 comments that fell within our charge.

And so there were general comments about privacy and security, and this is moving onto the next slide, and so the gist of the general comment was it is really vitally important that privacy and security measures are applied whenever patient health information are accessed and these should be applied in a manner that's aligned with a patient's privacy expectations. So that's the very high-level kind of general comment.

And then moving onto additional general comments that we received in terms of privacy and security, so we heard about a general kind of concern for healthcare organizations that were going to expose a public-facing API, so an API where patients could access their data from anywhere in the world. So, the general concern was about security and configuration, and hosting, and maintenance of these services in a secure way.

There was a concern that exposing an API like this could increase sort of the surface area for attack. So, it would increase the chance of a successful security attack and that could have an impact on the healthcare organization and also on the Apps that would be accessing the data through these APIs.

And then there was a general concern that providers and institutions today sometimes struggle to deal with the security configuration issues as managing SSL certificates and monitoring access to their services and generating alarms when services are available, handling things like maintenance and, you know, managing misuse whether it's intentional or unintentional. So, there is some experience on the ground today and all systems struggle to implement those kinds of features on the ground today.

And then we had some comments that were really implementation specific comments about privacy and about security. So, one is that an API might not need to include a means of establishing a trusted relationship.

So, for example, when patients are signed into patient portals that relationship can be managed within the confines of a known entity, which is the patient, and that is to say the patient might manage the authorization, the API access that's specific to them. So, we might not need something new in terms of managing that relationship.

And then there was a comment about some language that I haven't used yet in summarizing the certification criterion that is something called a patient's "token" which is an area of the certification rule that I think probably isn't entirely clear to most folks looking at this. I know it isn't to me but there is a notion of a token which is sort of a kind of patient identifier.

So, the comment was that querying for a patient's token is one means of selecting a patient but it's not the only means or shouldn't be the required means because there are alternative ways to select a patient as well. You might select a patient by passing an identifier or simply asserting what their identity is and then depending on the circumstances and the sort of interactions and the trust relationships here there might be particular ways of selecting a patient that makes more sense in one context or in another. So, that was really about the language on querying for a patient's "token."

And then one more slide with implementation specific comments. So, one comment here was, there were multiple commenters who suggested that OAuth or a combination of technologies that included OAuth, OpenID Connect and User Managed Access or UMA would be standards that would be relevant and useful for authentication and authorization.

And then a comment that the HTTPS has found wide success for application layer APIs and that as a general principle it would be good to have APIs accessible through HTTPS because it's so widespread.

So, that's a summary of the comments that we got in the public comment period before the publication of the final rule and I know that we're just closing out a comment period of the final rule as well. So, I imagine that during the course of our Workgroup activities we'll see more comments on the final rule will emerge and I think we'll probably have an opportunity to review those as well.

So, let me pause here before turning it over to Meg to summarize the previous HIT Policy Committee recommendations and ask if there are questions or comments just around this public comment period around the last few slides that I've presented here?

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

This is Aaron Miri, one question for this group and I guess related also to the final comments, was there anything around continued education for the consumer or any other audience around the privacy and security rules?

A lot of what we discovered, especially in the other FACA groups with Transport and Security and others was just simply the misunderstanding around what the Regs actually state and don't state. So, I'm just curious if any of that came up?

Leslie Kelly Hall – Senior Vice President of Policy – Healthwise

This is Leslie, it was discussed briefly in the Standards Committee but again our scope is not the policy. We could...our scope is really around the technology recommendations, however, education is important just as a buyer beware kind of tag might be important. So, I think that although it's not in our scope it has been talked about in the Standards Committee and I would defer to Michelle on that.

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

Yeah, this is Meg and actually the next set of slides we're going to talk a little bit about those previous recommendations from both the Policy and Standards Committees. I don't know Rose-Marie if you want to comment specifically did we see any of those questions from the public comments or Aaron was it just important to you that the topic was some part of the discussion?

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

A little bit of both to be honest.

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

This is Michelle, so I will say that on the Policy side the Consumer Workgroup had made recommendations around exactly what Aaron is speaking to and there had been some work done in the Privacy and Security Workgroup as well but I will turn it over to Rose-Marie to add any additional context based upon the comments that were received.

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

Yes, thanks, Michelle, this is Rose-Marie. We did receive comments and we do have some documentation from the Consumer Workgroup that wasn't included...all the comments from the Consumer Workgroup and recommendations were not included in our slide deck but we can provide that information to Michelle to share with the team.

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

That's perfect, thank you so much guys, I appreciate that.

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

Thank you.

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

It would be really helpful to sort of, you know, I think it might...to put it this way, if we could assume some things about the consumer's knowledge of privacy and security responsibilities that they have without going into how they get educated in order to make progress that might be helpful.

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

Right and this is Aaron Miri again, to the context of my questioning of once we have some of that knowledge base I think it will help us form the technical...

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

Yeah.

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

Recommendations because we can assume that denominator per se and drive forward with recommendations that wouldn't make any assumptions without, you know, some validation there.

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

This is Drew Schiller with Validic, I just want to say, so, with regard to the current slide that's on right now, slide 18, the OAuth and HTTPS are, from a technical stand-point, very, very obvious recommendations that we should wholeheartedly support.

With regard to what was on the previous couple of slides related to public comments I think that, you know, by and large, you know, we as a group can really help overcome...these fall under, in my opinion, a lot of the auspices of, you know, perceived risk as opposed to actual risk and so I think we can really easily address a lot of these concerns as a group.

And one final point that I want to make and this is maybe...maybe this is obvious, maybe this is nuanced, but, you know, consumers are not going to be the ones who are actually like building an API. So my mom is not going to take the API credentials from her physician and like code something to get her records, right?

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

Right.

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

This is just to allow somebody else to build that so that she can then sign in and get access to her records in a secure way. So, I just wanted to outline that and like as we're talking about giving consumers access like consumers aren't...these aren't going to be consumer-facing APIs necessarily, these are going to be APIs that allow for consumers to easily access their data. I just want to make sure that we're aligned there.

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

Yeah, so this is Josh, I'll endorse that point as well because I think the 99.99% use case is exactly what you just said, but I do like to bring up the important issue of sort of the consumers who are also tinkers giving people access to the tools they need to scratch their own itch, you know, there's been a lot of great developments that come from people building just what it is that they need or, you know, what it is that their grandmother needs and so yeah, I think when it comes down to opening up these APIs it's

mostly for App developers but we'll recognize that some App developers themselves do consume healthcare and their families consume healthcare.

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

Yes, wholeheartedly agree, yes.

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

All right, with that let me turn over to Meg for a review of the HIT Policy Committee recommendations.

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

Yeah, thanks, Josh. This is Meg. So, the remainder of the few slides that we have just really kind of to talk about the framework, those who have come, I suppose, before us and included with our agenda in our slides today was a document that ONC created for us with some links to two committee meetings, one Policy Committee meeting, one Standards Committee meeting in May of 2015 and specifically includes transcripts, recordings and the slides just for our reference, but at a very high-level on slide 20 I'll talk a little bit about what those recommendations related to privacy and security risks associated with APIs were that we saw in that timeframe.

So, some of the high-level bullet points as far as the risks associated with this increased access to data, certainly the heightened security risks from the increasing numbers of applications connecting to EHRs, what was perceived as vendors unclear or incorrect understanding of implementation of privacy and security legal requirements, vendors inadequate or incorrect implementation as entity's privacy and security policies, use of App or device with weak security controls or use of App or device without privacy policy or with unclear policy or even with policy that shares data liberally with third-parties allowing broad uses.

The next slide, on slide 21, ONC...based off some of those recommendations ONC is already working with FTC and OCR to develop mobile health best practice guidance for developers around promoting protection of user data.

And the Policy Committee's Privacy and Security Workgroup really talked about this quite a bit in their recommendations to get in front of this and be useful for Stages 2 and 3 of Meaningful Use and as far as specifics around some of the guidance for the App developers, best practices for protecting privacy and security of information collected by the App and connecting with EHRs covered by HIPAA. So, we do know that this work is ongoing and it's an inter-agency effort with FTC and OCR so we should expect to see a fairly quick turnaround on some of that best practice and guidance.

The Security Workgroup also recommended, slide 22, development of guidance for patients, consumers and providers. So, Aaron I think this gets a little bit to what you were bringing up before around can we assume a certain level of education or what's the process to educate consumers specifically around what these capabilities are, so their recommendation included, recommendations for guidance included check lists for what consumers should look for in a privacy or data use policy as they interact with these technologies, mechanisms for consumers to prepare privacy policies across Apps and there is a note here, similar to the ONC's model PHR notice and the link to that is also included in the slide if you want to take a look at that it's the Personal Health Record Model Privacy Notice that ONC has drafted.

How to do a security risk assessment on patient App or device connections such as through the API including the extent to which a provider may reject a patient's request for electronic access due to a perceived security risk for the provider. So, we do hear that concern quite a bit and I think that the ability in our charge to talk about provider to provider and provider to consumer is really going to be helpful here because it is a very real concern of providers what happens or what their liability is once their data leaves, if you will, their electronic health record. So, that's certainly helpful as part of this guidance security risk assessment on what the provider could do if they wanted to reject that patient's request for access if they felt that it wasn't secure.

And then the extent to which a provider may reject the patient's request for electronic access in the absence of a security risk. So drawing that out a little bit further, if there is no security risk is there capability or what is the extent to which that provider can actually reject that request?

So, next slide on 23 a continuation of these recommendations that ONC and CMS should provide specific guidance to address the transmit related risks and in making VDT and APIs available to patients, that guidance should address when that liability for data shifts from the providers to the patients and the extent to which providers must make patients aware when patients take responsibility for protecting data.

Best practices for counseling patients on assessing and managing privacy and security risks and then the responsibilities of vendors to include in their certified EHR technology security safeguards specific to the VDT and/or API modules.

We also saw some recommendations on slide 24 that the guidance should also address technical approaches that vendors may take to further protect data and one example that they note here are the "just in time" notices before the download and transmit that a patient would be able to turn off after their first notice. The ONC should also act on prior recommendations for guidance around identity proofing and authentication of patients including family members, friends and personal representatives.

Then we saw on slide 25 the note for the timely guidance is needed and the call for exploration of a multi-stakeholder group develop a program that would evaluate these patient-facing health Apps and the Workgroup noted that privacy and security are important but certainly the usability and the clinical validity of these patient-facing Apps would be important to note as well.

On slide 26 the guidance should also address the effort to leverage the guidance developed by the federal government entities including ONC and CMS. And a note here that even voluntarily adopted guidelines such as industry code-of-conduct could certainly have some teeth because the ONC under its existing authority can enforce those voluntary best practices for those who adopt.

So, if you set yourself out as an entity that adopts a particular best practice, a voluntary code-of-conduct for example, then the FTC would certainly have the ability to enforce you're doing so. Then the evaluation effort could also enhance transparency about privacy and security practices so again, just a lot around that education and transparency.

Slide 27, the Workgroup overall recognized the use of both APIs and the view, download, transmit along with a portal, that the following things must happen. So, these are pretty critical bullets here. Adoption and implementation of the API related recommendations of the Policy Committee, Privacy and Security Workgroup, so what we had seen before, everything that we just talked about, educating small practices and hospitals about APIs and their privacy and security implications and that note goes all the way back to a 2011 policy transmittal letter specific to educating patients and their families accordingly, consideration of certifying additional functions such that APIs may be used for functions beyond the download and transmit, and the requirement that APIs are publically available. So, those were specifically from the Consumer Workgroup recommendations.

So, the main take away from this, you know, Leslie you can attest to previous conversations, certainly Aaron and Robert, that the privacy and security concerns around APIs certainly aren't anything new, so we have a little bit of a framework that we can launch off with as we start our discussions and really try to focus on what the current charge is. We do have some background materials that will help facilitate some of the discussion. So, any questions on those?

Robert Jarrin, JD – Senior Director, Government Affairs – Qualcomm Incorporated

Hey, Meg, it's Jarrin, so I guess I want to go back to one of the initial slides which talks about the charge for the group because I realize that the first two bullets deal with privacy and then the second one is security but the third bullet really is about identifying recommendations for the ONC to help enable consumers to "leverage API technology" to access patient data. That is very different than privacy and security from the first two bullets and from everything that I'm reading and, you know, the presentation that you just gave the slides from the recommendations from the Policy Committee a lot of this stuff is focused on, you know, helping to inform patients and consumers about the privacy and security aspects like if you go to slide 22 a majority of that guidance is, you know, the check list, mechanisms, how to do a security assessment, you know, honestly consumers for the most part, you know, are probably not going to be either savvy enough to understand that kind of specificity about their APIs and what they're using or really care, you know, to be blunt.

You know I may be wrong and I don't have any kind of scientific evidence to prove that but from the patients that I deal with, you know, that's not, you know...and I'm not a doctor, I'm not saying that I am, but I do deal with a number of people that ask for help in advocacy, you know, I just don't see that this is an issue that they care about.

But that third bullet that I want to go back to that's closer to your slide 27 where you talk about consumer choice and use and I think that that's a really important aspect and that's why that third bullet to me is very different than the first two bullets that deal specifically with privacy and security, you know, enabling consumers to leverage an API technology to help them understand what is an API, how it can extract data from an existing electronic health record, how they can then access that data, you know, whether it's going to be through VDT or PGHD, or even secure messaging, etcetera, that's a very different charge.

So, I'm just kind of throwing that out there for you and for everybody else to discuss because I don't really see a focus on that. I see a bigger focus on the privacy and security stuff.

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

So, I'll...this is Meg, I'll take a stab, I agree Robert and then Josh and certainly Rose-Marie can jump in and clarify. I think the value of having this third bullet is to recognize that our privacy and security discussions around APIs are just going to naturally lead toward, you know, if we're talking about the perceived concerns that maybe fall outside of what we think are the real concerns then I think ultimately that's going to be what we start building that third bullet off of the education around what folks could perceive as a privacy or security threat that we can kind of get in front of and allow that bigger broader discussion to happen.

I know that we want to be very focused on what this Task Force is able to do, but it's such a broad topic, security and privacy when you talk about perceived and real that if we don't have that third one that allows us to really get into what is necessary for the consumers, the consumer aspect of it you're exactly right, you know, their education...then I think that our conversations maybe over in two or three meetings.

So, I do think that this was the point, the objective and the value of having that third bullet there is to allow our conversations to go there and allow our recommendations to kind of carve out where we felt focused on that additional education and guidance could be helpful. And then Josh I don't know if you have anything to add to that or Rose-Marie?

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

Yeah, I mean, this is Josh, on my side I think we sort of do our best to try to navigate between what is a relatively narrow charge on the one hand but then even within the charge itself we could see that we open up to broader issues about what enables consumers to leverage technology. And I think to the extent that we can provide concrete advice back to ONC about how to make this work, you know, we'll be acting within our charge even if sometimes we're going beyond strict sort of privacy recommendations.

**Aaron Seib – Chief Executive Officer – National Association for Trusted Exchange (NATE)
Right and I...**

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

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

And this is Rose-Marie, I completely agree. Some of the more specific consumer related items will be considered out of scope but will be addressed if it has to do with privacy and security since a lot of the consumer related items could affect our work but just to focus in on privacy and security was what our charge is and so we do recognize the fact that we would have some out of scope consumer items to review or put in a parking list for future work to be done on that, however, the third bullet was to capture the fact that we should address consumer access because it's an important piece to our rule as well as to MU.

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

This is Aaron, I just, I think it's also valuable because it points out a tension, right, that it will exist where we have different individuals who have different risk assessments and different preferences with regards to how they access and what are the requirements to access and the cost to access, and, you

know, I think the country is looking for some folks to help explain what that continuum might be and what is a tolerable minimum for all of us.

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

This is Drew Schiller at Validic, if I can just ask a clarifying question and forgive any naïveté on my part. Who would be the ultimate implementer of the API? And what I mean is as a consumer would I be accessing, you know, the Stanford API to access my Stanford patient data or would I be, you know, engaging with the EPIC API to access my Stanford information?

I think that there is a...the reason why I ask the question is because building and supporting, more importantly supporting, an API is not straightforward or without expense and so I think as part of the recommendation we should understand, you know, what we would be really looking for these end organizations to do and certainly having a technical support organization as part of supporting and maintaining an API. So, I'd just like some clarification around that.

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

So, this is Josh and I think you asked the question just perfectly.

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

Yes.

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

And the answer, I don't think we have a perfect answer, but the answer has a couple of parts at any rate and it's reflects, for better or for worse, the structure of the regulatory environment. So, when it comes to who has an obligation to provide patients with access to their data, you know, the answer is pretty clearly it's the covered entity.

And when it comes to who is the target of the Meaningful Use Incentive Program, well it's the healthcare providers, it's the eligible hospitals and eligible providers who are participating in the Meaningful Use Program.

So, from that perspective, you know, it's my hospital, it's my doctor who is offering these APIs to me but of course if you look one level deeper my hospital and my doctor's office has to use a certified EHR product in order to offer those APIs to me and so there is an EHR vendor responsible for that certified product.

And I think in most deployment environments it is going to make a lot of sense for hospitals and clinics to outsource some or probably all of the work of exposing those APIs out to the vendors, so that is an App developer. It is possible, I might just connect to one environment for a particular vendor in order to test my application into their software stack or maybe they'll want to white label different copies of that environment for different healthcare organizations. I think that's going to be part of the business planning and the marketing of these organizations to figure out what works. But from the consumer perspective I'm connecting an App to my data at a particular hospital or clinic. Is that a fair sort of description of the landscape?

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

Josh, this is Aaron, I would just, you know, you used the word “as an App developer” and the question I want...that I think we’ll be clarifying is, are you in that role an App developer for the consumers or are you an App developer for the covered entities, or are there two species one that is an App developer for providers and one that is an App developer for consumers?

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

Thanks, Aaron, so the picture I had in my head was somebody building an App that consumers will use and it maybe that consumers are my opening target audience or maybe I’m building a tool that’s just going to help consumers share healthcare data between two different hospitals.

But in any case the picture I had in my head was somebody building consumer-facing Apps and tools. When it comes to somebody building provider-facing Apps and tools I think we actually have a very similar story.

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

Yeah, I think there is a lot of commonality, you know, when they are a covered entity that we can rely on some of the guidance and the, you know, historical information that we have about how HIPAA covered entities must comply.

But from the perspective of a consumer-facing application developer that’s where it is less clear to many people that are, you know, working in that space. If they must meet a minimum what is that minimum. If they can offer things that exceed that minimum how do they ensure that the APIs that are standardized for covered entities will interact with them and so on and so forth.

Robert Jarrin, JD – Senior Director, Government Affairs – Qualcomm Incorporated

So, this is an important conversation, this is Jarrin again, because, you know, for any consumer API to exist the API developer is going to have to engage with the EHR company directly which will be engaging directly on behalf of the covered entity. So, I don’t see it as you know...I mean, yes there’s a distinction but at the end of the day I think that any developer, any API developer is going to have to be transacting with both the consumer side and also the vendor/ultimately the covered entity. Am I incorrect in that assumption?

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

I don’t think you’re incorrect but I think that there is, you know, some layers that are less hardened that we’ll discover over the next couple of months. When we talk about, and it’s come up in the bullets so far, consumers being able to compare and select consumer-facing applications based on their privacy and security offerings that I think is...and maybe I’m wrong, but I think that this is different where I kind of had this expectation that might be entirely wrong, that at the end of the day the privacy and security requirements on the covered entity side are well-defined or at least better defined than on the consumer side because on the consumer side there is the notion of the individual consumer having a choice on, you know, which of the spectrum of security components they require so on and so forth where they’re taking the risk and the liability no longer exists on the part of the covered entity.

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

Yeah and I think as we dig into these issues over the course of our Task Force, you know, we’ll discover that one of the challenges here is a covered entity may be providing these APIs, maybe exposing data for consumer-facing applications.

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

Right.

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

And we might try to say, by the time the data feeds into the consumer application the covered entity has no responsibility for it anymore, it's the consumer Apps responsibility at that point once it's been handed over. But merely by hosting a public-facing APIs for authorized users to access the covered entity is increasing its surface attack or attack surface, it's making it easier for nefarious parties to come in and pull their network and I think that interface is where we'll start to see some of the real concerns emerge which is I want to expose enough data through the right interfaces so that consumers can exercise their right to access but I don't want to open up my network to, you know, various kinds of probing or attacks from the outside world and how do you balance those two factors.

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

Right and this is Aaron Miri again, as a CIO of a covered entity let me offer up that even if technically we could and we want to, believe me we are a cutting edge 21st Century hospital that we believe in pushing the envelope and sharing data and open notes and all those sorts of things, working through the legalese and working through the interpretation of the HIPAA Regs and those sorts of things sometimes the answer is no simply because of the fear factor and if you look at a number of HIEs and even PHRs and others that have failed across the country it's been that folks are just too scared to move.

So, again, I go back to, I think it is important we address this issue because I do think that the general landscape you have organizations or covered entities that do want to move the ball forward but again there is a frightened nature about the way we go about our business.

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

This is Aaron I'll just say "ditto" yeah I totally...there is a paralysis and, you know, a gap in interpretation or if someone is looking for, you know, guidance on...that would be a huge output of this kind of Task Force.

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

Yeah, this is Drew Schiller, I wholeheartedly echo that, in fact Jarrin's earlier comment about what is the common clinical dataset, I actually tried to look it up and found the relevant documentation so I could say "oh, well, common clinical dataset is this" it's mentioned 157 times on the federalregister.gov page and I still can't figure out what it is. So, not...

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

Thank you for saying this. This is Aaron I've felt...

Robert Jarrin, JD – Senior Director, Government Affairs – Qualcomm Incorporated

Welcome to our world Drew.

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

Yeah. I just thought I was dumb and I couldn't figure it out.

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

Well, at least you both figured out that the only possible way to read any of these documents is through aggressive use of search, search and count. So, I know that in wrapping up today's inaugural call we do have to leave time for public comment at the end. Before we open up for public comment is there any additional discussion or issues that we want to raise for the group?

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

Josh, there's a lot of links in the slides, in the presentation when you download it and on slide 24 I have a very specific question, slide 24 it links to a PDF and I guess my question is, the recommendation from the HIT Policy Committee was that the ONC should act on prior recommendations for guidance on identity proofing and authentication of patients. Is this PDF the pointer to that prior recommendation that we should be looking at or is there a different document being referred to in that bullet?

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

Is there someone from the ONC group who could answer Aaron's question?

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

Yes, hi, Josh, this is Rose-Marie, yes the PDF is where that guidance is located.

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

All right.

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

And it's on healthit.gov so that particular document will have these two recommendations listed.

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

The May 22nd recommendation, got it, thank you.

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

You're welcome.

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

Their recommendation is a recommendation of creating...guidance it looks like, okay, great, thank you.

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

All right, other questions or comments before we move into the public comment phase?

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

So, Josh, this is Meg, maybe just one, so I know that next week's call we're going to be chatting a little bit about the virtual hearing talking about the goals and the outcomes so, slide 30, so maybe just a head's up on that if you have any thoughts around what that hearing should look like some of the types of questions we will be going through that next week so just something to...a little bit of homework I suppose to think about over the next few days.

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

And Meg could you...

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

And...

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

Define a virtual hearing? What that entails and what specifically we mean?

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

So, it's, I'm trying see here on the work plan, if we were to go back to that. The later part of January, so the end of January, the 26th and the 28th the Task Force will be hosting a couple of virtual hearings so...and Michelle I'm sure that you've explained this so many times you know it by heart, but basically what we'll be doing is creating a list of questions that we would like specific types of panelists and specific panelists themselves to speak to us a little bit about, so it's sort of an educational aspect of it and that will inform our final recommendations that we...and that drafting for the April timeframe. So, it is just really to kick that off.

We'll have a few phone calls or a few meetings where we can refine it just a little bit better, but just wanted to give a head's up to the group that we will begin talking about that. So, if there is anything that you're thinking about, any particular topics that you want to make sure that we invite someone to speak to us around how APIs are used or how specific privacy or security problems are amplified through particular use cases we could certainly start those conversations.

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

Whose brains we want to pick and about what.

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

Yes.

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

Thank you.

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

So, Michelle, does that cover it pretty well?

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

I think you did a great job, thank you, Meg. Okay, it sounds like we're ready for public comment?

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

I think so.

Public Comment

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

Lonnie, can you please open the lines?

Lonnie Moore – Meetings Coordinator – Altarum Institute

If you are listening via your computer speakers you may dial 1-877-705-2976 and press *1 to be placed in the comment queue. If you are on the telephone and would like to make a public comment, please press *1 at this time.

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

So, while we wait for public comment our next meeting is actually this Friday, December 4th at 11:30 Eastern Time and it looks like we have no public comment. So, thank you all for joining our first meeting, this was a great lively discussion and look forward to future discussions.

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

This is Aaron I just wanted to...

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

Thanks, everyone.

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

Thank Josh and Megan.

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

Thanks, guys.

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

Thank you.

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

All right, bye.

Ivor Horn, MD, MPH – Medical Director, Center for Health Equity – Seattle Children’s Hospital

Thank you.

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

Bye.

M

Bye, have a good day.

Robert Jarrin, JD – Senior Director, Government Affairs – Qualcomm Incorporated

Aaron are you still there? Aaron, hello?