

HIT Standards Committee Final Transcript October 21, 2011

Presentation

Mary Jo Deering – ONC – Senior Policy Advisor

Good morning, everybody. This is Mary Jo Deering from the Office of the National Coordinator. Welcome to the 30th meeting of the HIT Standards Committee. This is a public meeting. There will be an opportunity for public comment at the end of this meeting, and I would ask all members to identify themselves when they speak, both for our listeners and for the transcription. I'll turn it over to John Halamka.

John Halamka – Harvard Medical School – Chief Information Officer

Good morning, everybody, and thanks for joining the virtual meeting. I wanted to, of course, recognize all the hard work that you have put in from April to September by giving you a little less travel in October. Dr. Perlin will be joining us shortly, we hope. He is working on some aspect of his day job. So I will kick us off. Today's meeting is really an opportunity to polish the work that we've presented in September as we do some additional refinement, and we're going to hear three presentations. Dixie will be presenting the work of the Privacy and Security Workgroup as it tries to present the certification criteria after a thorough review of privacy and security implications of some of the Meaningful Use Stage 2 desirable policies, and today it is really presenting those to us as a group, but it's really part of a process which goes through the Implementation Workgroup. So lots of opportunity for review and discussion, and I presume then, Liz and Judy, you will incorporate those in the grid and then give us a brief final report out.

One interesting challenge about the work that Dixie's group has to do is we know that standards sometimes for content and vocabulary can be quite concrete, but when we cover privacy and security sometimes there are functional characteristics, and so as you go through and ... your presentation what is this balance between specificity of an exact method to secure data versus functional characteristics and desirable qualities because we know there are many ways that our organizations, large and small, will want to secure data. So I think she's had a very, very good discussion among her workgroup and a good balance on all those issues.

We're going to hear an important update from Doug Fridsma on the S&I framework and some of the work that it continues to do, which I think will also give us additional work as we think about our meetings in November and beyond. For example, when I think of standards, we've talked about there are contents, vocabulary, and transport standards, on the content side the work on consolidated CDA is so important, and Wes will make some comments during that discussion. The consolidated CDA provides a level of specificity that cleans up and refines and removes some optionality from the C32 document. I exchange hundreds of C32s every day and to do that across our community has required that Massachusetts write its own more specific implementation guide that further constrains what is a ... script that has been used for Meaningful Use Stage 1. Consolidated CDA really cleans up a lot of the optionality in C32, so we'll hear from Doug about that work and hopefully its acceleration.

We'll also hear about reportable lab, and as we think about laboratory one of the things that I think we'll probably have to deal with in the future is the compendia. We've talked about this many times, but as we get more and more refinements of that lab transaction not only is it important to say it's HL7 2.5.1 and here's exactly how it's going to work for simple and complex use cases, but making sure we have the

vocabulary so that as interfaces are built the most common lab tests are in a compendia that everyone can reference, making the cost of laboratory interfacing as inexpensive as possible.

One other issue that Doug will touch on is the issue of the NwHIN, and we together, just last month, looked at what are those low risk standards, where are areas that we need some additional effort and simplification. And so hopefully we can all engage in a discussion as to where can we refine and enhance those NwHIN exchange specifications, what are our opportunities for hearing additional testimony from those in the industry that have implemented the NwHIN exchange specifications, because we've got a lot of testimony as part of the initial process but I think we've heard there are more people who'd like to come forward and talk about their experiences. Are there opportunities for us to launch, either through the S&I framework or one of our own workgroups, a way where we can look at some of these RESTful techniques that are so commonly used in Facebook and Google and Amazon and are there ways that RESTful approaches could refine some of the NwHIN specifications on the exchange

Also something that Doug will reflect on, we have not, together, thought about image transmission. We've thought of course about HL7 messaging and summaries and vocabularies and transport, but how is it that from a radiology result standpoint we consider the text or the image. What about new cloud hosted Web-based approaches for image sharing, or DICOM being a somewhat extensible standard, are there constraints that should be placed on it so that image sharing is more simple, it's today got a lot of variation. That's not been in any of our workstreams to date, and as we move to our future stages of meaningful use thinking about that is going to be important.

Then we'll hear an important update from Steve Posnack on the comments on metadata ANPRM, and recognizing there that as we think of the whole package of everything we've done imagine I take an HL7 2.5.1 message or a consolidated CDA summary, well, how do I get it from point A to point B? Maybe the right answer is to say here is your payload, wrap it in the metadata CDA R2, wrap that in a transport mechanism, as we've talked about, XDR, SMTP, S/MIME, the direct standards and send that to another location, the advantage being with the metadata wrapper you don't have to go into the payload itself to figure out what patient this may apply to. So we'll hear some comments from many stakeholders about those metadata standards and should they be part of Meaningful Use Stage 2, should they be piloted, what are the next steps? Along this discussion today I think it is important we reflect on what I just said, on pilots, where are there pilots of certification criteria, pilots of some of the newer emerging standards we've looked at, pilots of the metadata, so that the Implementation Workgroup can collect industry experience and make sure that all of us feel good about moving forward based on industry experience. Even though the standards look great, in reality are they great? So hopefully we can accomplish all of this today in just three hours and look forward to the discussion.

Mary Jo Deering – ONC – Senior Policy Advisor

John, this is Mary Jo. I neglected to take the roll. So I didn't want to interrupt you, but if this is the time you were going to turn it over to Dixie, could I perhaps take the roll?

John Halamka – Harvard Medical School – Chief Information Officer

Well, in fact, in previous meetings we do the preamble and the roll taking, so you are right on track and I'm turning it back to you.

Mary Jo Deering – ONC – Senior Policy Advisor

Well, thank you very much. I appreciate that. Okay, I'll run through the members, and please let me know if you're present. Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I'm here.

Mary Jo Deering – ONC – Senior Policy Advisor

Anne Castro?

Anne Castro – Blue Cross Blue Shield South Carolina – Chief Design Architect

I'm here.

Mary Jo Deering – ONC – Senior Policy Advisor

Aneesh Chopra? Chris Chute? Janet Corrigan? Tim Cromwell?

Tim Cromwell – VHA – Director of Standards & Interoperability

Good morning.

Mary Jo Deering – ONC – Senior Policy Advisor

John Derr?

John Derr – Golden Living LLC – Chief Technology Strategic Officer

Present.

Mary Jo Deering – ONC – Senior Policy Advisor

Carol Diamond?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Here.

Mary Jo Deering – ONC – Senior Policy Advisor

Jamie Ferguson?

Jamie Ferguson – Kaiser Permanente – Executive Director HIT Strategy & Policy

Here.

Mary Jo Deering – ONC – Senior Policy Advisor

B.J. Lide for Cita Furlani?

B.J. (Bettioyce) Lide – NIST – Scientific Advisor for HIT

Here.

Mary Jo Deering – ONC – Senior Policy Advisor

C. Martin Harris?

Martin Harris – Cleveland Clinic – Chief Information Officer

Here.

Mary Jo Deering – ONC – Senior Policy Advisor

Stan Huff? Kevin Hutchinson? Elizabeth Johnson?

Elizabeth Johnson – Tenet Healthcare – VP Applied Clinical Informatics

Here.

Mary Jo Deering – ONC – Senior Policy Advisor

Rebecca Kush? David McCallie?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Here.

Mary Jo Deering – ONC – Senior Policy Advisor

Judy Murphy?

Judy Murphy – Aurora Health Care – Vice President of Applications

Here.

Mary Jo Deering – ONC – Senior Policy Advisor

Nancy Orvis? Marc Overhage? Wes Rishel?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Here.

Mary Jo Deering – ONC – Senior Policy Advisor

Cris Ross?

Cris Ross – LabHub – CIO

Here.

Mary Jo Deering – ONC – Senior Policy Advisor

Walter Suarez?

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

Here.

Mary Jo Deering – ONC – Senior Policy Advisor

Sharon Terry? Karen Trudel? Jim Walker? Okay, thank you, John.

Stephen Ondra – NeHC – Senior Policy Advisor

And Steve Ondra is on the phone.

Mary Jo Deering – ONC – Senior Policy Advisor

Thank you, Steve.

Floyd Eisenberg – Siemens Medical Solutions – Physician Consultant

Floyd Eisenberg for Janet Corrigan.

M

....

John Halamka – Harvard Medical School – Chief Information Officer

Okay, well why don't we go ahead and proceed with Dixie's work on looking at the certification criteria for privacy and security.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Thank you, John. Today I'm representing the Privacy and Security Workgroup and presenting our recommendations for certification criteria, standards, and implementation specifications for Stage 2 Meaningful Use. This is our response to the assignment that you heard from Judy and Liz at the last meeting, when they presented the Implementation Workgroup's work on Stage 2. Would you proceed to the next slide, please?

These are the members of our workgroup, and I thank all the members for their work on this. It's been very aggressive on a very short time line, but I think we've accomplished quite a bit. Next slide, please.

This is just reminding you of the process. The HIT Policy Committee presented their Stage 2 Meaningful Use objectives and measures and other directions and in our case other directions included a number of policy recommendations from the Privacy and Security Tiger Team that operates under the Policy Committee. At the last meeting of the Implementation Workgroup Liz and Judy presented their work on Stage 2 and they requested inputs from the Privacy and Security Workgroup on both privacy and security related objectives and measures and also objectives and measures having to do with patient or consumer communications. And in some cases the spreadsheet or table that they gave us they had already done some work and made some suggestions, and in those cases we considered their suggestions in our own work. So we reviewed all of the measures and suggestions and today I'm presenting our recommended certification criteria, standards, and implementation specifications. The complete recommendations are included in the appendix to the presentation today, so I won't go through every line in excruciating detail, but I will tell you a summary of the ultimate recommendations. Next slide, please.

As we did this work, an issue that has been an ongoing challenge for us, again, came up, and that is how can we really assess what security functionality should become security certification criteria for a complete EHR or an EHR module. Basically, if you look at an enterprise the most effective security measures and the most effective assurances, which are confidence that those measures are actually working, the best ways for protecting electronic health information are really built into the infrastructure. They're not built into each application individually. They're built into the overall system architecture fundamentally. Those are the foundational protections. They're built in the operating systems that the applications run on. They're built in the database management systems.

And there are a number of third party specialized services that applications typically use rather than do everything themselves, such as enterprise identity management is very common, audit monitoring and misuse detection, audit integration, and audit reduction, and management often is done as a service separate from the applications themselves, virus detection, public key infrastructure, how much of this should really be criteria for the EHR certification versus assumptions of the infrastructure, and yet we don't want to really assume that all of this is here. So it's a very difficult challenge. But we all agree that EHR technology should depend primarily upon these infrastructure assurances and specialized security services and that the EHR itself should provide only those security services that are specific to protecting the confidentiality, integrity, and availability of electronic health information that it manages, and of course any additional security services that are not provided by these third party services and infrastructure components. Next slide, please.

This recommendation, as captured on this slide, we consider the most important of all of the recommendations we're making today. The Privacy and Security Workgroup actually made this recommendation at Stage 1 as well, but we want to reiterate it because we do continuously deal with it and have discussions around it and it's a challenge for us, and I'm sure it's a challenge for vendors who are submitting their products for certification as well. But fundamentally effective integration of EHR infrastructure and these specialized third party services is key to protecting electronic health information

care quality and patient safety. And today during Stage 1 every complete EHR and EHR module is required to meet all security certification criteria. And this approach tends to encourage the implementation of security services within each EHR and each EHR module, rather than having the EHR use the stronger mechanisms that are provided by infrastructure and third party services. So to enable the certification process to more effectively address security integration, both the integration of the mechanisms themselves and the integration of the EHR in an environment that provides higher assurance, we recommend that the ONC and NIST consider modifying the certification process so that each privacy and security certification criterion is treated as addressable, much like the HIPAA security rule considers a number of its implementation specifications addressable.

But in the case of privacy and security, to meet each criterion, each complete EHR or EHR module that is submitted for certification would need to either implement the required security functionality within the product that they're submitting for certification, or assign the function to a third party security component or service and then demonstrate how the certified EHR product integrated with these third party components and services meets that criterion. Again, we believe this general recommendation is extremely important, so I would like to pause here and encourage any discussion of this recommendation before I proceed with the more detailed recommendations.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Wes Rishel. In general I think the point you're making is extremely important and you really are headed in the right direction here, but I have some questions. First of all, without actually reviewing a list it's not clear to me that every security or privacy recommendation should be addressable. I assume that we'll see more details later on. For example, there are requirements for role-based access and so forth that seem to require a rather intimate relationship with the EHR software in order to be issued. So I'm just wondering if case by case there might be a few where addressable isn't appropriate. I'm specifically concerned that there are multiple products adopted site by site to provide security, for example, antivirus products, and I'm not sure that what we gain in certification testing, would we pick one of the products that some sites use and certify with that. Would they have to certify with all of the certification, all of the antivirus products that any of their clients could use, or is this something that really needs to be addressed in the required HIPAA site audit rather than in a recommendation for the certification of the EHR.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Wes, as usual, these are really good points, excellent points. I would personally answer the first one is that I think that you're probably right that there may be some that should be required to be implemented in the EHR, but I would emphasize maybe. I think that's a tough call, because even the one that you mentioned, role-based access control, it depends on how the EHR is integrated with the system. It could be integrated with the operating system in such a way that each user is known to the operating system in which the operating system could enforce the role-based access control. It could be integrated with a database management system, in which case the DBMS could provide role-based access control. So given that example raises questions and I think as technology matures there will only be more questions. I think that that's a really good point, but I'm not sure that it actually can be done and I think that ONC and NIST should certainly consider that as they consider our recommendations, but I think it's a tough one.

The second one I also think is extremely tough, the multiple security products, whether the NIST and ONC selects one or more or how it's done, I don't know. But we feel it's very important that they reconsider this approach rather than continue to require that each module and each product implement every single criterion.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

And with that I agree 1000%. Just a couple of quick statements on your reply, I'm thinking that there's a need to categorize criteria into those that are expected to have a solution that is certifiable, and by that I mean that the standard environment for the EHR that is used for certification includes the modules necessary to provide those security functions. So, for example, you mentioned the authentication through the database or through the operating system, well, that's part of the standard EHR module, it doesn't vary from site to site. But many other certification criteria, such as intrusion protection, antivirus, things like that, really are only addressable at the site level; the vendors expect different sites to use different products for those. Those are the ones I think that are most appropriately put into a meaningful use criterion rather than a certification criterion.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

Cris Ross – LabHub – CIO

I'm sorry, Dixie, this is Cris Ross. Do you want to respond to Wes? I didn't want to interrupt.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

The assumption that you mentioned that, well, the operating system is part of the certification, even questions about whether the operating system provides a particular certification criteria, the operating system, that is part of the certification, even questions about whether it be the application or the operating system were raised in our discussions, so this is a tough issue. You mentioned a good approach, but clearly I think we all agree it needs further discussion, but I think it does need attention. Cris?

Cris Ross – LabHub – CIO

Dixie, I agree, and this line of comment is really interesting. My only question and comment I guess is that some of the things that we're talking about here seem familiar if you've been through a SAS 70 or a Sarbanes-Oxley health IT or IT audit in the separation of what things can be vendor adjusted and what things need to be attested by site. Your workgroup has clearly done lots of great work here and you're, I'm sure, terribly familiar with this, but did you look at patterns from things like best auditing practices from SAS 70 and Sarbanes-Oxley to try and figure out where to draw these lines?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

No, no. I certainly appreciate that and I'm sure that ONC does as well. I'm not familiar with those practices, but it certainly sounds like something that should be considered. That's great. Thank you, Cris.

Cris Ross – LabHub – CIO

After living through them in several environments, I can say that I'm having a sense of déjà vu that may be useful.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

This is great. Are there other comments? Okay, let me go on to the specific recommendations, if you would advance the slide, please. This slide has to do with the consumer communications recommendation. The table that was given to us by the Implementation group had some of these, especially ones that came out of the Tiger Team, they were listed under Privacy and Security, some of them were listed in patient portal type recommendations and we considered them altogether and we also recommended that they be considered altogether when the regulation is being put together, all of the privacy and security criteria that have to do with consumer communications. So all of these are new for Stage 2, none of these were in Stage 1, so the first one is really the result of Tiger Team action is that the

Tiger Team recommended at least one single factor authentication for patients to authenticate themselves to what they call the patient portal and what we call a consumer Web-based application. But basically single factor authentication that is not required beyond single factor but it requires at least single factor. The Tiger Team did not advise that they disallow two factors, but they did recommend that it be at least single factor.

Secondly, the ability to exchange messages securely, and we broke this down into certification requirements to authenticate the consumer, presumably using at least single factor authentication to authenticate the EHR itself, the identity of the EHR itself, to encrypt and protect the message itself. The standards that we recommended were FIPS Pub 140-2, which is part of Stage 1 for exchanging electronic health information, transport layer security, which is the protocol that's commonly used for Web-based application security, and the third standard we recommended was secure e-mail, SMTP, S/MIME. The implementation specifications we named were the NIST Special Publication 800-52, which is TLS, Transport Layer Security, and the NWHIN transport specifications. Another security criterion was the ability for the consumer to securely download health information. That should be "securely" not "security," securely download information. The Tiger Team recommended that it include data provenance with the downloaded information and we don't have standards, so we didn't recommend any standards in this area. But we did recommend that as a criterion.

Then the last one that came out of the Tiger Team was a warning before PHI was downloaded by consumers, in other words the consumer would say I want to download my health record and then the system would come back and say, are you sure you want to download this PHI here with some of the risks? And we recognized that this could be significant impact on existing products and so we recommended that the Standards Committee go back to the Policy Committee and recommend that that be made guidance or best practice rather than a certification criterion for products. Next slide.

These are, we're moving now from the general privacy and security requirements. We recommended no changes for the existing certification criteria in the areas of access control, accounting of disclosures, general encryption, which is just what algorithms should be used, and accounting of disclosures, which I listed twice. Next slide, please.

The recommended changes, I have a couple of slides here. The first one is that the Implementation Workgroup actually in their comments back to us said that this criterion was posing some challenges to the certification team in that it wasn't clear the existing certification criterion really uses the words that are in the HIPAA security rule itself and the phrase that the HIPAA security rules uses is the ability to terminate a session. So questions arise around whether terminating a session is putting the user device into screen saving mode and locking out the user until they come back and enter their password to get back in, or does it really mean terminating the session and automatically logging them off. Well, we considered this and we concluded that, yes, it means both.

So we specifically recommended separate criteria around this that the certified product be able to lock a session after a designated period of activity, in other words, go with a screen saving mode where you have to enter your user ID and password to unlock and that they also be required to do session termination, which is automatic log-off, after a designated period of inactivity, and that they have the capability for a system administrator to designate separate periods on inactivity for session locking and termination. In other words, what we're saying here is that users, perhaps after let's say five minutes the screen would lock, but it wouldn't completely shut down their session. And then maybe after two hours, and I'm just making up these numbers of course, it might completely log the individual off. By having the capability to designate these time periods it gives each site the capability to designate the time periods for their particular, and it could be role-based or whatever.

The second general area of change was audit log, and there were some recommendations from the Implementation Workgroup around this as well. They recommended changing the title to activity auditing, and we agreed. We recommended to broaden the scope to allow more selectivity for security auditing. Right now if you go to the audit log standard certification criteria and standards you'll see that the certification criteria requires the ability to audit events, and that the standard itself is an enumeration of specific events that should be audited. We felt that the product should provide the capability to audit security relevant events, but deciding exactly which events the EHR product should be auditing should be site specific, just like as in HIPAA. HIPAA allows each enterprise of covered entities to specify exactly which security events are auditable. So we recommended that the criteria say that the product must detect and record information about security relevant events. This is another thing the existing criterion says that the EHR must audit actions related to electronic health information only, and we felt that there are more security relevant events that should be part of the certification process, just actions related to electronic health information, and we even debated about what actions related to electronic health information actually are.

The second criterion that we're recommending is to change the standard itself from this enumerated list to record audit data about security relevant events. And then we're recommending adding, as an implementation specification, ASTM E214701, which is a document specific for healthcare and it includes enumerated lists of both security relevant events that they recommend be considered for auditing and also, by the way, includes a second list about those events that should be considered for accounting of disclosures. But we felt that that would be a good list to refer them to in selecting those security relevant events that should be auditable. Then the Implementation Workgroup suggested adding audit data protection provisions and we agreed with that and recommended that as well. Next slide.

The Implementation Workgroup suggested we consider changing Secure Hash Algorithm, SHA-1 to SHA-2, but there are many, many products and protocols actually that don't yet handle SHA-2. But we agreed that we should be encouraging people to move to SHA-2 because it is stronger than SHA-1 and so we recommended adding SHA-2 as a standard but retaining SHA-1 as a standard as well.

Under authentication, right now the authentication standard is exactly what's in HIPAA and it says it requires the authentication of every person and entity, and we recommended separate criteria for person authentication versus entity authentication. For person authentication we recommended at least single factor authentication, and for entity authentication we recommended the use of digital X.509 digital certificates, which are what is used in both the Direct protocol as well as the Exchange protocol. And they're also used by TLS protocol so they're generally in the S/MIME, so they're generally used for entity authentication quite commonly.

In the encryption area, as I mentioned earlier, the general encryption standard we recommended no change. But we recommended that the criteria incorporate the provisions of the document that the secretary issued as required by HITECH around breach notification provisions. The HITECH said that the secretary should recommend guidance specifying technologies and methodologies that render protected health information unusable, unreadable, and indecipherable to authorized individuals, and organizations that use those methods to encrypt data that are on devices that are then breached, they have what is called a Safe Harbor so they don't have to notify HHS of the breach because everything is encrypted and they don't have to notify each individual because everything's encrypted. That document that was issued by the secretary includes some very specific requirements around encryption and we felt that they should be incorporated into the certification criteria.

First of all, we recommended adding the criteria for encryption for data at rest. The overall objective and measure for security specifically calls out data at rest, encryption of data at rest. It says two things, it says you conduct a risk assessment and you encrypt data at rest, or address encryption of data at rest. The secretary's guidance refers specifically and only specifically to data at rest for end user device storage, so our recommendation was that EHR technology, whose functionality includes the capability to manage electronic PHI on end user devices, must be able to encrypt and decrypt data that are persisted on those end user devices. In other words, if the EHR writes data to an end user device and then uses that data and actually manages and controls those data that are written to the end user device, then that EHR should be able to encrypt and decrypt the information on the end user device.

The second was encryption when exchanging electronic health information, which is an existing criterion, but we suggested we align it with the secretary's direction and add TLS and IPsec, Internet Protocol security, which is used for network level virtual private networks, and that we add the implementation specifications that are cited for breach guidance plus the NwHIN transport standards themselves. Next slide, please.

These are new objectives and measures that were introduced. These were already listed on the materials that were given to us by the Implementation Workgroup, and they got them from the Policy Committee. As I mentioned, the overall objective measure mentions encryption of data at rest in data centers and mobile devices, and we recommended that encryption for data on end user devices that are controlled by the EHR be part of the certification criterion that I just discussed. We felt that encryption of data in data centers is a risk management decision and we feel that it is out of scope for certification criteria, which is consistent with what was suggested by the Implementation Workgroup, and we agreed with their assessment there.

Two factor authentication, we agreed with the Implementation Workgroup's assessment as this is out of scope, in particular because we were advised by Steve Posnack that DEA is already addressing their requirement for two factor authentication, so we don't want to either duplicate what they're already doing, and we don't want to do anything that's out of sync with what they're doing, so we felt that it was out of scope here. Entity level digital certificates, we incorporated that X.509 certificate in the entity authentication criterion, the Tiger Team recommended the ability to detect and block programmatic attacks, that's their term, but they describe that as meaning the lockout after an allowed number of log-in attempts. There are a number of technologies that are used to share authenticated identities these days, SAML is one of the common protocols used, ... is used, and Open ID, or all the single sign-on kind of approaches as well, so we felt that the ability to lock somebody out after an allowed number of log-in attempts really doesn't align well with how identity is measured today. And so we suggested that this committee suggests the Policy Committee consider this as guidance or perhaps best practice rather than as policy.

Then the final topic that we addressed was amendments to help records, and this was on our list but this clearly is not uniquely privacy and security. But we tried to interpret the requirements to recommend some certification criteria, but we really strongly recommended that the Implementation Workgroup have an expert in medical records review the criteria we suggested. The ones we suggested were the amendment by authorized provider while preserving data integrity, the attachment of patient assertion and provider rebuttal, and providing an audit trail from amendments. All three were derived from the HIPAA policy rules so this topic really should be reviewed by somebody that's knowledgeable in medical data records. I think that's the end, but would you go to the next slide.

Again, this is just a reminder for me to tell you that detailed recommendations are in the appendix, which Mary Jo just distributed with the presentation.

John Halamka – Harvard Medical School – Chief Information Officer

Great, Dixie. Thanks so very much. Dixie and I had a lot of dialogue about as I introduced her topic where do you have specificity that becomes certification criteria, as in NIST would build test scripts and look at the detailed performance of a module or EHR with a test script versus where is it addressable out of functional characteristics. Dixie, one quick question, for ASTM E2147, do you see that as a set of best practices or do you see that as something that would actually result in NIST building some type of script to test functionality of a module or complete EHR?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Great question. I'm really glad you ask it, John, because this is one of the outstanding questions that the Privacy and Security Workgroup really doesn't have the answer to and we struggled with is that we know that the existing regulation includes certification criteria and standards, and it makes it pretty clear that if you want your product certified you meet this criterion and you use this standard or this choice of standards. The existing certification criteria, or regulation, does not include implementation specifications at all, and initially our workgroup thought, well, implementation specifications should be guidance documents on how to implement TLS, or how to implement secure e-mail, but that it wouldn't dictate a solution. So if you had a particular implementation guide you wouldn't necessarily have to meet the criterion using exactly the method described in that implementation guide.

And then John told me that it was common that what was in the implementation guide was then used to derive test scripts for certification. And in that case I think we probably would even make some changes to these recommendations if that is really how the implementation specifications are used. Actually, the 21407 has a list of auditable security relevant events and that document does make a number of those optional, it doesn't say do everything, one of these, it says the following are essential and the next three are optional kinds of things, so it provides some optionality, but that's not always the case. So I think in the case of 21407 it's probably pretty straightforward. I think other implementation guides are less straightforward, so we certainly are reaching out to ONC and asking for clarification on how the implementation specifications are actually used and what they really should be. Are they really as strong as the standards, or are they intended to be guidance in how to implement the standards and certification criteria. So I've answered your question with a question, John.

John Halamka – Harvard Medical School – Chief Information Officer

Do we have a representative from NIST on the phone today?

B.J. (Bettijoyce) Lide – NIST – Scientific Advisor for HIT

Yes, I'm B.J. Lide representing Cita.

John Halamka – Harvard Medical School – Chief Information Officer

Could you comment on, again, we want to try to be as specific as we can, but at the same time recognizing if so much security is addressable this is a question that probably NIST and ONC getting together and chatting, what is the difference between a best practice versus an implementation specification that results in an actual test script and conformance testing?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

We have commented on this, our security folks have, Kevin Stein, and we would be happy to continue discussion with ONC, this committee and others to make sure that happens.

John Halamka – Harvard Medical School – Chief Information Officer

Very good. Other questions or comments on Dixie's work?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Wes here.

John Halamka – Harvard Medical School – Chief Information Officer

Wes, go ahead.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Dixie, whenever I hear about optionality I have a reflex action, my foot comes up and kicks me in the head. The SHA-1 and SHA-2 recommendation, does that affect interoperability? If one certified EHR vendor uses SHA-1 and another certified EHR vendor uses SHA-2, are they unable to interoperate because of each qualifying by a different standard route?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

It depends. Where this will mostly be affected is in the use of transport layer security because not all TLS implementations are capable of using SHA-2 yet. The way TLS works is the handshake at the beginning, the side that's trying to connect tells the other side the protocols that it supports. So if it only supports SHA-1 it will send over and say SHA-1. If the other side only supports SHA-2, then it would pose a problem. In general the other side is more likely to support both and they would have to agree upon, because the first step is to agree upon what encryption and integrity –

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

....

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

... they will use. So they have to agree upon it and they have to be able to both support SHA-1.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Would it be better to say that the options are SHA-1 or SHA-2 and SHA-1?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, I agree with you. Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Thank you. With regard to logs of events, particularly ... related to users accessing protected health information, you mentioned already I think the NPRM for accounting for disclosure that carries with it a strong assumption of the level of auditing that's being done in the EHR with regard to this issue. Is your recommendation consistent with that NPRM, which is not a final reg of course? Specifically, I think it would require an audit log that included the identity of the user, the identity of the patient, and some general information about the purpose for which information was accessed, not so far as to say whether it was for printing or not, but just very general.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, that is consistent with the ASTM 2147, but we recommend that they not specify exactly which data elements must be required in the certification criterion. The policy, that's really a policy in each organization, would need then to go in and specify these are the events that I'm going to audit because the accounting for disclosure policy requires that I have that information. The approach we're recommending is that policy drive the enterprise's decision on what data elements to audit.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Yes, I understand, and I think that's appropriate. With regard to certification –

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

They need to – yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

... however, if you certify certain things then you know that it's possible for policy to require that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, I know exactly what you're thinking. How do you suggest we handle that?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

My own opinion is that there's potential for significant variation between the final rule on accounting for disclosures and the one that has come out. But the common sense notion of the level of auditability that's required in it, it seems that those minimum criteria should be certifiable. The logic of the regulator right now in the accounting for disclosures NPRM is that this is a low cost requirement for the industry because every EHR that is legal under HIPAA already does this. I think that that's a faulty assumption at this point and I think we can help close the gap by allowing for a wide suite of auditable events, but picking a minimum number of auditable events that are consistent with privacy protection and requiring certification of that much. Again, it's up to the site to set the policy for what it does.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

There are two things that you specify. There are the events to be auditable and there are the data elements that are collected per event. The items you've mentioned, like the users, the patient, and general information about the disclosure are really elements to be included in the data for the event. So it may be that we should specify the data elements to be recorded per event but not specify the events.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

That's a possibility, and I know that it's a pretty complex set of options there. It's not immediately clear to me that you can specify auditable elements entirely independent of – no, I said it right the first time – data elements entirely independent of the audit events because there are audit events, such as attempts to access the system, that may not yet have established a user ID or a patient ID or things like that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Right, right.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

But all I'm saying is that as this has worked going forward the notion that there is some minimum amount of audit that is likely to be necessary in order to meet other HIPAA based regulations should be a consideration in reaching your final decision.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

That's a good point.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Now, in that regard, the definitions of EHR in that regulation and the definition of EHR that we use under meaningful use are different, and it seems clear that there is a requirement implied in the accounting for disclosure NPRM for merging audit logs produced by multiple systems in order to create a consolidated report of access. I don't know what the ASTM standard does in terms of formatting of the audit log itself. Does it provide a standard format? Would ATNA be an alternative? I don't have a specific suggestion here. I'm just raising issues that have come up as I've talked to clients about this.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, actually we discuss ATNA quite a bit because that profile does address the merging of audit records, and the existing certification standard is nothing but here you must detect events and you must record information about those events, and it says nothing about the merging of audit records. If there were a certification criterion about the merging of audit records and audit reduction and audit analysis, there's clearly a need for further work on both standards and implementation specifications.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Okay. There are many areas in technology where common sense is both required and extremely dangerous, and security is one of them. So when I argue from common sense here I want to pull my punch, but the general notion that good security and good protection of private data requires correlation of information across multiple applications within an enterprise seems pretty strong and if we can encourage EHRs to produce their audit information in a format that is mergeable, then I think that's worthy of some consideration.

Going back to your prior section about encrypting data at rest, I think you and the committee have done a good job of addressing the single most important issue, which is end user devices considering that they're getting smaller and smaller and easier to lose all the time. I was not clear about what your recommendation would imply about a browser cache, so if I am using a tool that is in fact browser-based on my iPhone or brand X phone, is there a requirement that the HTML or whatever language is being used to drive the user interface on this device include provisions to clear the cache or not? And I think it's something that ought to be considered at some point.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, I think the way we worded it, it said that if the EHR controls the information from the end user device, which they do for cache, and they have to be able to encrypt any data that are persisted. So if they cleared cache the data are not persisted. If they did not clear cache then they would have to be –

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

The way you just stated it I think is fine. I possibly didn't quite get the words right when I heard it the first time. It's clear you've already considered the issue. That was my most important concern.

John Halamka – Harvard Medical School – Chief Information Officer

Thank you. Carol Diamond is also in the queue. Carol, please go ahead.

Jim Walker – Geisinger Health Systems – Chief Health Information Officer

Pardon me, John; Jim Walker. I joined about five minutes ago.

John Halamka – Harvard Medical School – Chief Information Officer

Do you also have a comment on this topic?

Jim Walker – Geisinger Health Systems – Chief Health Information Officer

No, I was just instructed to notify you that I had joined.

John Halamka – Harvard Medical School – Chief Information Officer

Great, well welcome. Carol, please go ahead.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

I just wanted to clarify something in the interchange between Dixie and Wes and also clarify the objective of the recommendation, particularly in the area of access control and audit. I understand why using the certification process to make sure that there is the capability to do these things is important. I also

understand inside of an organization the virtues of merging, for instance, audit records. What I'm confused about is whether or not these recommendations and these standards are made on the presumption that there is interoperability of these capabilities across entities, and if so why?

John Halamka – Harvard Medical School – Chief Information Officer

This is an excellent question, and Dixie and I actually have had this discussion already, so Dixie, could you comment on that?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I'm not sure what she means by interoperability. Across organizations or across systems?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

In other words –

John Halamka – Harvard Medical School – Chief Information Officer

....

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Go ahead, John.

John Halamka – Harvard Medical School – Chief Information Officer

What she's referring to is the discussion we had about ATNA and the architecture and do you impose a specific architecture on the auditing process. The example that I gave, Carol, was I have 146 different clinical systems, each of which produces an audit trail containing data elements, but those data elements are actually in a different format and structure, sometimes ... audit trail, sometimes I have Web services, I have all kinds of different audit trails that I combine into my security monitoring systems. But the vendors, if told there's only one way to produce an audit trail in an architecture would have massive reengineering to do and the question is, is that something that we want to impose, and I think, Dixie, you had a sense of no, actually.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Right, but my question is actually at an even higher level than that, which is to say I understand when you're in a large integrated system you have some of those challenges, John, but I'm actually coming at this from the very simple view that a single office that's using an EHR needs to use an EHR that has the capability to do these things, but derives little value from the work that's necessary if what we're recommending is there has to be a standard specified for how that information is collected and stored internally.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

The criteria, I want to back up a bit. The certification criteria that exists today say nothing about the merging of audit records, either between an organization, and I don't know of a case where you do merge audit records between an organization –

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

I don't either. That's why I'm asking.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

And I agree with you that a small practice that has one system, it's EHR, there's no need for the capability to merge audit records. I think that the merging of audit records and consolidation across the large enterprise, I not only think, I know, it's beyond the current criteria as they exist today. In the future we don't have any criteria that say the audit records must be mergeable. Now, Wes has suggested that the

audit records be collected in a standard format so that they are mergeable. I question even that at this point for exactly the same reason that John pointed out, there are even commercial products that specifically do take audit records from multiple platforms in however they collect it and bring it together in a normalized format so it can be reduced and analyzed for intrusion detection as well as misuse detection. There's a whole industry that does exactly that without requiring that audit records be in a standard format. But the existing criteria don't address this topic at all.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Dixie, can I –

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Hold on one second, Wes. I just want to clarify, Dixie, that the recommendations that we're making are really about implementation specs that would get certified to demonstrate the capacity for the EHR to do this, not the capacity for the EHR to collect and store the information in a certain data format.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Right. The criteria that exists today requires the EHR to do four things. Number one, detect security relevant events. Number two, record information about each of those events. Number three, protect the audit trail so that nobody can go in and modify it or delete it or overwrite it. And number four is to generate some kind of report on the auditable events, security relevant events for that EHR.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

So the recommendations, the implementation specs that you recommended, the ASTM and the NIST recommendations that you make, those are recommendations for the EHR. I'm not familiar with either of these specs and didn't have time to look at them, but these are specs for EHR's capability.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, and I think, let me see, yes, I am right. I wanted to confirm before I said that, the only implementation spec that we've recommended for audit is ASTM E214701, which has a list of auditable events.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Okay, and leads the data format and the – I'm just trying to avoid an unnecessary requirement for work that in terms of writing to a specific standard that doesn't have a big payoff.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, it does not recommend a particular format or messaging protocol. It really lists the auditable events.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Okay, thank you.

John Halamka – Harvard Medical School – Chief Information Officer

So, last word on this, and then we will move on to Doug.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Sure. Carol, I think has raised some excellent points that I hadn't considered in my comments. In Dixie's response I understood her to allude to a set of requirements. I'm not sure what is the provenance of those requirements; is it the law, is it guidance from the Policy Committee, or what? The only thing I was trying to inject is the likely requirement, as evidenced by a notice of proposed rulemaking, for the ability to account for access, to create an accounting for the patient of access to information across the HIPAA definition of electronic health record, which is broader. And that's not a requirement, you can argue,

because it's not a final rule. So I guess I don't have much of a leg to stand on here. It does strike me, and I wanted to say that when I said ATNA I did not mean to imply the entire services definitions associated with ATNA, I meant to imply only the log format.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Wes, I think that your comment about making sure that our certification requirements are consistent with the accounting of disclosures regulation, I think that's a great recommendation and it's completely consistent and compatible with what Carol said as well, because even with respect to accounting of disclosures, if it's a small system it still may not need to merge the records to do that. But I personally agree with you that the certification criteria or the methods that they certify systems, that we make sure that they are consistent with the accounting of disclosures regulation. I think that's a really good point.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I wanted to add one last comment on why this merits the attention we've been giving it. You mentioned that there are a number of commercial tools available for compiling security events from multiple systems for various kinds of security analysis, one of which might presumably be accounting for accesses. I looked into those tools in reviewing the other NPRM and what I found is those tools are characterized by a lot of custom code for major high-end applications packages to get the non-standard log outputs into a standard format, and they don't, by any means, automatically easily or even possibly cover all of the applications in an enterprise. So the benefit of having at least a nucleus of the audit log that's important for accounting for disclosures in a standard format is pretty high and the cost for a system that already produces the data in some format to produce it in a common format is not as high as going in and changing the internal auditing of the system.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

That's useful. Thank you.

John Halamka – Harvard Medical School – Chief Information Officer

Thank you. The three administrative items, Mary Jo, so we have now heard from Dixie and had many comments. I presume as a next step we will forward ... comments to the Implementation Workgroup, who will incorporate it into their matrix and presumably then at our next meeting make a couple of comments and seek formal approval. Is that the right process?

Mary Jo Deering – ONC – Senior Policy Advisor

I believe that's the right process, and we have Steve Posnack on the phone, who is the recipient of these inputs. Steve, does that jibe with your understanding?

Steve Posnack – ONC – Policy Analyst

Unfortunately, no, to be clear. It would be best if the Standards Committee felt that it was appropriate to recommend Stacy's workgroup recommendations for ONC's consideration and merging with the Implementation Workgroup. As previously mentioned with the Implementation Workgroup's recommendations, these are starting points for the rulemaking process and valuable feedback in terms of the recommendations and approaches that we can take with refreshing and crafting some of the new certification criteria that would be necessary for the next rulemaking. If the comfort is there to go ahead and do so, with all due respect to Liz and Judy, you have done a tremendous job, they have other things that are on their plate, and I'm not necessarily sure I see the need to go back and get another workgroup to sign off on something that's specific to the area that Stacy's workgroup is responsible for.

Judy Murphy – Aurora Health Care – Vice President of Applications

This is Judy Murphy. I would absolutely agree. And I know the time crunch that we're under, which is another reason probably why Steve is saying we have to act now and he needs those recommendations now. If you remember at the last Standards meeting he was reticent to even give us the time that we took on this, so I think we have to just go forward from this point and give those recommendations directly to Steve for consideration in the NPRM.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Judy, you and Liz can say, yes, we approve.

Judy Murphy – Aurora Health Care – Vice President of Applications

Yes, we approve.

John Halamka – Harvard Medical School – Chief Information Officer

Why don't we ask it this way, Liz and Judy, I was just trying to be respectful for you, so if you have given us your approval let me ask the Standards Committee are there any objections with approving these recommendations we have received from Dixie and the associated comments as guidance to ONC? Well, no objections being heard and with Liz and Judy –

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

John, I had my microphone on mute. The only objection I have is the language around SHA-1 and SHA-2 that Dixie took that into account and I'd like to see that change in the final recommendations.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, I agree with Wes, yes.

John Halamka – Harvard Medical School – Chief Information Officer

We will forward those recommendations to ONC, and, Steve Posnack, we have met your deadline.

Steve Posnack – ONC – Policy Analyst

I thank you all. Dixie and Walter did a great job I think channeling the group's energy, so very much appreciative of their efforts in the past couple of weeks.

John Halamka – Harvard Medical School – Chief Information Officer

Mary Jo has also reminded me we have not approved the minutes. And so if folks on the call have had a chance to take a look at the minutes of our last meeting were there any edits or changes to those minutes recommended?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

This is Carol Diamond. I have a slight clarification to a comment, which I'll e-mail to Mary Jo.

John Halamka – Harvard Medical School – Chief Information Officer

Great, thank you very much. With that one amendment we will accept the minutes. And then, Mary Jo, you also wanted just to ... if anyone has joined the call, Jim Walker, I know has joined, are there others who have joined the call?

Doug Fridsma – ONC – Director, Office of Standards & Interoperability

Doug Fridsma is here.

John Halamka – Harvard Medical School – Chief Information Officer

Great. Okay, Mary Jo, any other administrative items?

Mary Jo Deering – ONC – Senior Policy Advisor

Thank you very much.

Stan Huff – Intermountain Healthcare – Chief Medical Informatics Officer

John, this is Stan Huff. I was slow hitting the mute button. I also joined about 15 minutes into the call.

John Halamka – Harvard Medical School – Chief Information Officer

Okay.

Mary Jo Deering – ONC – Senior Policy Advisor

I am wondering if Marc is here, because his plane was supposed to touch down by 9:30. Marc Overhage, are you on the line? Okay, he must be still airborne. Thank you very much, John, I'm done.

John Halamka – Harvard Medical School – Chief Information Officer

Okay, very good. Well, let's move on to Doug. Doug, while you were not on the call I actually had introduced your presentation and described that there were some very important S&I framework updates that you would be making, specifically around what additional work is being done on consolidated CDA, what additional work is going to be done on NwHIN exchange refinements, getting additional testimony, and then the notion of looking at some of the imaging standards or the text associated with an imaging report. The one thing I also mentioned, which I know is not specifically in your slides, is you have focused on the lab use case for simple EHR reporting and complex lab data exchange that we also reflect on compendia that might be used for ordering labs. It's just not something we've addressed yet, but certainly it's something that a lot of work has been done. So let me turn it over to you.

Doug Fridsma – ONC – Director, Office of Standards & Interoperability

Thanks so much. I certainly appreciate it. This is intended to really be an update on some of the standards efforts that have gone on since the last time we had a meeting and to queue up, as John has said, some questions that I think we may not resolve today but certainly I think it would be useful to have a plan going forward about how we might get some input or get some discussion or come to some conclusion. So if we can go to the next slide.

The first thing that I wanted to say is that we have completed this week the second of our Standards and Interoperability framework face-to-face meetings, and I wanted to give people a sense of where we are within the S&I framework. We are a year into standing up the activities within the Standards and Interoperability framework and so we're being somewhat reflective within our office to try to take a look at what's working and what's not working and how we can, after a year, refine the process and make sure that we still remain targeted and lean and agile in all the things that we think are important. The face-to-face meeting occurred on October 18th through the 19th. We had a total number of people registered of 284 people, and attended 234, so we had a very large turnout of people, all coming together and sitting together in rooms here in Arlington to go over some of the projects, both those that are nearing the end trying to determine lessons learned, trying to figure out how we can proceed and provide advice to the new activities that are starting, working on some coordination mechanisms across the different initiatives. When we were one initiative it was easy, when it was three it was manageable, and now we're getting close to nine and so we really have to be thoughtful about how we can maintain the good synergies across programs as well.

I think the other thing that's important to note is that we currently have about 885 registered users that are participating in the Standards and Interoperability framework. As I said last month, it's humbling to see the amount of enthusiasm and just the expertise that's coming together to help solve many of the problems that are going on. Of those I will say that there's probably about 400 or so that are really active

participants and that are on many of the calls. I think the remaining number of people are tracking and monitoring and trying to stay connected but may not be actively participating. But the reason that that's important is that of those 400 that have been active participants, a significant number of them were able to attend the face-to-face meeting, and I think we will probably in the next month's meeting provide you some of the feedback and the synthesis of that meeting. But I wanted to give people a chance to understand where we are right now within the Standards and Interoperability framework now that we're coming up to our one year anniversary. So we'll go to the next slide.

As John had articulated, I think there's a couple of things that I would like to tee up for discussion and to make sure that we have an opportunity to either talk about it today or at least queue up some activities, give us some advice about how best to do things. I wanted to, first, start off again by thanking the NwHIN Power team for all of the incredible work that's going on. I think one of the things that is really important to tease out of the discussion that we had last month was that the teams really did a lot of thoughtful work in evaluating standards readiness and to examine the kinds of criteria that are really important that allow us to select between different standards to be able to triage what sort of work needs to be done, whether we need to focus on implementations of pilots or whether we need to focus on the SDO and standards processes. And so I would encourage us to continue that work on the criteria for evaluation and I think it provides a tremendous amount of transparency and it allows people to understand the processes that the deliberations occurred within the Power team and translate that into a way that people who may not be entirely steeped in all of the nuance of the standards can then understand. I think that's one thing that I would hope this committee would be able to move forward with, is to continue that work because I think it will be useful in a whole host of other places.

I think the second thing is that one of the things that I heard, and I think I've talked with some of the committee members as well, is that there were some people that believed that we need to get some additional feedback around the NwHIN implementations. We had very, very good engagement and feedback from a lot of the federal partners who have been active and long term users of many of those specifications. But there's also a number of people that didn't have the opportunity to provide comments, and I think one thing that will be helpful is to figure out how to do that, whether we should have a meeting devoted to it, whether we should try to solicit some written testimony to pull things back, but I want to make sure that we circle back and address that issue as well to make sure that we can be as inclusive as we can with the kind of feedback that we get.

The second thing to talk about is that I know that there's been a lot of discussion about what to do with some of the radiology standards, standards for both imaging and standards for imaging reports. We all recognize that images are an important part of the portfolio of information that physicians and providers look at in terms of making good decisions, and the question is, is that if we were to include something regarding radiology into meaningful use, what would be the kinds of things that would be useful to do and where is the current status of those standards, and what should we be looking at? Is there additional work that needs to be done? Are there other things that we need to do? Is there an incremental task that includes some of those standards?

Then the final thing, and I just want to go through the presentation, these are topics for discussion and I would hope that after we get through with some of the transitions of care and the consolidated CDA discussion perhaps we can come back to those things as well. The last thing, and this was a request, is to talk through in a little bit more depth the work that's gone on with transitions of care in the consolidated CDA project as part of the Standards and Interoperability framework. Let me just say that we have some of our key leads among the teams that have been supporting those projects that are on the phone. We have Rick Kernoff and Eric Pupojiten is also on the phone as well, and so those are going to be resources

that will be available to the committee if we need to ask some very specific or technical questions. We'll go to the next slide.

Just to remind folks about the transitions of care initiative, that initiative is focused on improving the electronic exchange of core clinical information among providers, patients, and other authorized entities in support of meaningful use. That team has been working on a number of activities, one of which was to develop a clinical information model that helps organize the information that would go into a care transition. This is something that we are really trying to understand the best way to do that, what's the right way to model it, what are the right ... to use, and it certainly isn't anything at this point that we are ready to promulgate or the like. I think we really are in an exploratory phase, but we understand that much of the good work that's gone on with Stan Huff and the work of HL7, the work in NIEM, all of those different projects really do rely on a separation of representing the kinds of concepts or the kinds of information that's important and getting that in a particular model that may be independent of whether it's representative of a NIEM IEPD, or whether it's representative of a V2 message or a V3 message or the like. We are working on that and the Transitions of Care team is really helping with that.

The thing I think that's important to recognize is that the Transitions of Care initiative has come up with some clear guidance on the usage of core clinical elements that they've identified in common care transition scenarios and they've reached agreement on a single standard for clinical summary documentations in support of meaningful use. They're also working very, very diligently on some implementation guidance, on vocabulary mappings, things about conversion tools that might be able to migrate existing implementations that use the C32 or CCD ways of describing that into a consolidated CDA standard. If we can go to the next slide.

This is a slide that we presented last month, but I just wanted to pull this up to remind people graphically what we tried to do. I think the thing that's important is that for Meaningful Use Stage 1 we had in those regulations both a C32 and a CCR as two standards that would be suitable to meet the requirements of Meaningful Use Stage 1. At the time we realized that there was a lot of optionality within the C32 and for the last year and a half or so we have noted in projects like VLER and NwHIN and others, that that optionality creates challenges for us in terms of getting to interoperability. So if something is optional for one group and the other group is expecting to see it, or they don't include that, we end up having to spend a lot of time negotiating how we're going to be sending this C32 because there are lots of different ways to do it and still have it conform to the standard. So the effort of the transitions of care initiative was really to take what I would say the flexibility of the C32 and all of the different nuances that you can have there, and the ease of implementation of the CCR and begin to take the best of both worlds, getting to the point where we've got a series of building blocks or templates that can all be put together to describe a particular transition and to do it in a way that has less ambiguity but still maintains a degree of flexibility in terms of being able to send things.

So as an example, and it's very simplistic and those of you who are very technical could question exactly that, you can help me nuance things out, but the issue is that suppose I wanted to send a transitions of care document from an emergency room to a primary care physician, and that was an important transition of care that we wanted to support, what we might find is that we need a template to describe basic demographics about the patient. We might want to include the template that says here is the medications the patient is on, here are the problem lists that they had, and here are the things that we decided to do as an action plan moving forward. But in the transition from the emergency room to the primary care we might include a template about procedures that were performed and we might include some other information about discharge planning that might be relevant. So you would have those core elements, plus a couple of extra templates that would define that transitions of care and really help someone say this is the way in which that transition should occur. Now, if you were sending someone from a primary

care provider to a consultant you might reuse or use the same template for the basic patient demographics, the problems that that patient has, and the medications, but you might include a template that says here's the clinical question that I'm trying to ask and that I want you as a consultant to answer, and I might include some laboratory tests or some imaging results or something else that says here is their most recent EKG and here is their most recent cholesterol panel, so that you have additional information when you evaluate the patient, and you may not include things like discharge planning or the like. So the idea of the transitions of care initiative is to try to create these building blocks, much like we've been talking about with other kinds of standards and transportation and messaging, to create those different building blocks that we can then assemble to provide both clarity about implementation but the flexibility of what pieces should be included. Can we go to the next slide?

There's a variety of things that we've been working on. First of all, from a functional perspective we've got a use case and a clinical information model that has achieved some consensus about what the functional scenario requirements might be and tried to capture those data requirements, or those data elements that need to be exchanged in this information model. That helps us describe at a high level concepts like we know we need to have a patient that has a first name and a last name, we know there has to be a collection of diagnoses, we know that there are medications that are going to be important, and we describe those in an information model at a relatively high level and then that allows us to translate that into the more technical details without having our medical experts who are part of the transitions of care getting caught in the weeds around XML.

The use case also provides clear guidance on the usage. One of the things that's important to interoperability is to use the right implementation guide or the right standard for the right purpose, so getting clear guidance on how to use a particular implementation guide or particular standard helps us get closer to that interoperability. So one of the things that I think transitions of care did very well is to try to create some clarity around that. I think the other thing that they've done, and we're using the term consolidated CDAs, is that we've had very good participation and working relationship with the HL7 community as well as members of the IAG community, who serve in a capacity across both HL7 and IAG, to take a look at the current challenges that we have within the way in which CDA works, and then try to come up with a single common catalog of reusable templates for components that are the building blocks that we can assemble. So in that example that I gave around the emergency room, this notion of taking the demographic section or laboratory section and a medication section, those would be examples of three different kind of reusable objects or reusable components that could be assembled together. The group has achieved, in the participants there, agreement on a single standard for what those clinical summary documents would need, what are the kinds of building blocks that would need to be included in that. I think that's an important aspect of the work that's gone on within this group and that is moving the ball forward with regard to interoperability. Next slide.

I think this is the last slide and then I think we'll be able to open it up for discussion about this and then if we have time maybe go back to some of the earlier questions that we had asked. From a technical component there's a lot of stuff that we're trying to do under the hood to make this simpler, both from a developer's perspective and an implementer's perspective, as well as from a use perspective. One of the things, and we've talked about this from the very beginning and this is our first foray of getting into that, we're trying to transition from paper-based or document-based descriptions of what these standards should look like, to ones that are based on computable models, or things that computers can manipulate and we can then develop tools that will help us with things. We are using something called UML, unified medical language, that helps us describe these things in ways that a computer can understand them, and the thing about that is if we want to describe it so a computer can help understand it, it requires us to be unambiguous and it requires us to be able to be very precise in how we describe things. This is the underpinnings of what our information models would look like, and we're experimenting with some tools

as well that will help with implementation. We're developing some prototypes of conversion tools that would help migrate people who are using the traditional C32 guides around what a CDA document would look like so that they can move over to this consolidated CDA that has those building blocks that can be assembled. We're developing what we would call a reference implementation, because oftentimes programmers do better if they can look at something that works and then modify it for their purposes, and so this notion of a reference implementation that will help people understand precisely how the specification should be interpreted we think will be also helpful in terms of getting implementations out there as well.

We're also trying to figure out how can we assist people in looking at this and getting to this simpler thing, and so we're developing some educational resources within the Standards and Interoperability framework and within this team we're working on testing that we think hopefully will help with conformance testing so that we can begin narrowing down the specificity with the tools. And we're doing that in conjunction with NIST, and so in support of this notion of moving from having documents that describe how to implement a particular standard to models that computers can understand, it's sort of like rather than having a Word document that describes how to implement each of those building blocks we have a database that has the elements of those building blocks and we can then query it and we can do all sorts of things with it as a result. So we've been collaborating with Open Health Tools and with the VA to develop some tools that allow us to take a model of what the standard should look like and have it automatically generate the document that is the specifications. So it knows the way in which the standard is then developed and how it's been modeled within these tools, and by hitting a button it's like it writes the specifications for you.

So we've been working very, very hard because, I said this all the time, which is standards are standards because people use them, and so part of the efforts within the transitions of care project is to actually put together the resources and the tools that will allow people to get there faster by having tools that will help educate them, things that will make it easier for the developers of the standards to make sure that things are consistent across different projects, and getting good implementation guidance that includes not only the syntax but also vocabularies and vocabulary mappings that need to be included.

So with that, I'm going to stop with the presentation. I've given you a tremendous amount of fairly technical information but I think the question that I was trying to address is as we think about this transitions of care document how does it relate to what's gone on before and what is the path forward toward success if we want to converge on a single standard that is easier to implement and that will move us closer to interoperability. So with that I'm going to stop. I'm sure that there's a whole bunch of cards that are up, so I'll turn it over to John.

John Halamka – Harvard Medical School – Chief Information Officer

Thank you very much, John. We have about half an hour for this discussion, because we knew it would be rich to follow along on your S&I presentation, really three topics, consolidated CDA, next steps on NwHIN, and starting to think and plan about what we might do on radiology and DICOM. And I know there are many cards up, but Wes had said to me last evening a set of comments that I think are so relevant to this last point you made about consolidated CDA. Wes, would you like to make those comments?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Thanks, John. I did want to ask Doug one question, which is that the consolidated CDA, as I understand it, represents a much broader scope than C32. C32 is a continuity of care document. There are a number of user stories that have been addressed separately, including continuity of care in the CDA. Is

the intention through transitions of care to make all of those stories part of the certifiable content for EHRs or specifically the continuity of care document?

Doug Fridsma – ONC – Director, Office of Standards & Interoperability

And that's a great point, Wes, you're right, the consolidated CDA is actually a much broader initiative than just focused on transitions of care. But one of the things that we wanted to do is to test whether or not this approach using these building blocks and trying to constrain the set of templates a little bit more, whether or not that approach worked we wanted to be able to test it, and so transitions of care as a project was a good vehicle to focus that energy and make sure that we've got at least those elements and to see whether this approach would be useful.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Okay, thanks. Just to qualify, there are really three levels of generality I think we're talking about. The first level of generality is the CCD, which was really, to the best of my understanding, designed for a specific transition of care, or a set of transitions of care that falls short of all transitions of care. For example, the scenario of ED to the primary care physician or ED to a specialist might include things that wouldn't be included in a just physician to physician transition of care across offices and things like that. There are several user stories; the same user stories, as I understand it, specific transitions of care. Then there are other user stories that may not even be about transitions of care. I think it's just important for the industry to understand out of the consolidated CDA which ones they figure they should be gearing up on for Meaningful Use Stage 2. Obviously until the reg is final you can't say for sure, but there are ways I think to provide guidance that the industry would find valuable.

I'm going to go into the prepared material, which was written before I heard your testimony, so in some cases you'll say, oh, we already did that, and that's just great. I spent the last week at the Gartner Annual Symposium, and we had a very good turnout of healthcare folks at it this year, including a number of people who had worked on dealer and on other C32 based implementations. And I've had some e-mail discussions over the same period of time, and what I heard about implementing the C32 in general is that there is a very large amount of debugging that goes on at implementation time, and particularly that the sources of the problems are that the current C32 requires simultaneous interpretation of a number of documents and that the XML expressions, which are called XPATHs, that define where data should be placed in the XML document are in terms of abstractions so that even an experienced programmer may have some difficulty deciding which one of these abstractions relates to which piece of data identified by a business name in their particular system. So when there are multiple interpretations or as programmers tend to do under deadline, there is pick one and we'll figure it out on debugging, that the obscurity of the XPATHs is an issue.

I think people are also discovering ambiguity, where information that is not required or optional may go, so the testing tools tend not to comment if information is put in one place or another as long as they both are valid XPATHs for data. And as a result, if you take two CCDs created by the same document and display them, you either see data in different fields or data missing even though it's in the XML document because the mapping into the system was looking in one place and the sender was putting it in another. There are also differences in handling text such as when text is a comment or when it's permissible to send either text or structured data for a given data item, at least one implementer of the CCD had decided well, we're only interested in selected data and structured data so they had stripped out comments about tests that were clearly important for the clinician to see in reviewing the test results.

The people that I've been talking to for the most part have been working on the consolidated CDA project and they are really very happy with the result, they think that HL7, working with other organizations, has done a tremendous job to flatten the specifications into a single document, and although it's not straightforward to at least provide the business names associated with the XPATHs and make them accessible. I think HL7's done a wonderful job in pulling this together, getting it done, and I think ... and ONC has done a tremendous job in terms of cutting through a number of organizational issues with HL7 and other organizations, making it possible to produce a consolidated CDA.

Many of the people I talked to felt that this specification alone will prevent as much as half of the programming errors that are found in C32, and furthermore will cut the staff time spent in debating the interpretation of the specification down substantially. When the specs are difficult to interpret various people can each feel they have a valid interpretation and with no real appeals court to go to they have to argue it out and it will be a lot easier arguing it out based on the consolidated CDA. There's another opportunity to increase the efficiency of programming and testing again when the business names are actually used in the XML, so this notion of to relate a business name to a fairly arcane XPATH goes away. This could happen through the detailed clinical modeling work that's going on or if greenCDA becomes accepted as a wider format, that would provide the same capability. I still see some important opportunities that ONC and NIST need to do to further reduce the amount of bilateral testing that will be required when trying to exchange a document that will contain some mixture of structured data and text among EHRs.

It would be ideal if two EHRs that were certified interoperated. In fact, there are probably many user organizations that would expect that of certification. I think that's more than we can achieve in this round, but quantitatively we should be able to make a substantial reduction in the bilateral testing that's required for interoperability. The measures that I recommend are, one, – can people hear me over the music here?

Operator

Yes, we're trying to pinpoint the music and delete it.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Okay, thank you.

M

It improves you, Wes, it's great.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Well, yes, however I could completely clear the phone just by trying to sing along with the music. Everybody would hang up. So the things that I think need to happen are testing interoperability not only by seeing whether messages pass parsing and Schematron evaluation, but actually looking at the data in the system after a message is received, looking at the data in the system before a message is sent, and see that the correct data is associated with the correct business name. I will point out that this is the testing level of certification as required both for ePrescribing and for lab data by the specialty organizations that are responsible for making sure that data is interoperable, and it's required at implementation.

Another important thing would be to use multiple test scripts with different business values for structured data, not defaulting to a single simple case. For example, in one area of testing where the NIST test goals were used the only test for microbiology was no growth detected. Well, when there's no growth there's no additional susceptibilities that are ordered, there's no sustained alternatives, there's no reason to believe that two implementations of microbiology, both of which handle no growth the same way, also handle all of those other things exactly right. So a much richer set of test scripts around variations in what are normally acceptable business values is required.

The third thing is I'm not going to try to suggest an organizational way to do this, because though I think I understand the square root of two and Pi, I have no idea how the government works, but somehow funding a public testing tool that uses the same testing rules that will be used for certification, of course with different specific data, a tool like that should use parsing and Schematron testing with a post processor that identifies the business names of the data items associated with errors, right now those errors are reported in terms of the arcane XML names. And too, provide sample messages with displays

of the business data that they contain so the developers can test their inbound processing. One of the hardest things to do during the actual time when people are moving toward demonstrating Meaningful Use Stage 2 will be to deal with issues that really haven't been discovered in the standards process, and an example of that might be a rule out diagnosis. Right now there's apparently discussions going on that lead to three alternative ways to represent a rule out diagnosis, which effectively means there is no How would the industry deal with discoveries of these kinds of topics as they come up? I think that we should be looking at some sort of best practices council that can discuss those. That council wouldn't, in any way, be able to guarantee the HL7 would finally decide to implement the way they recommend it, but at least it could get us through Stage 2 and give HL7 the time to do its level of discussion that's necessary to do good work.

I did a quick back of the envelope calculation with some of the people that worked on VLER, and we very conservatively believe that if you count the number of EHRs who have been certified and think of each of them as a separate development effort you could save \$25 million in costs by implementing these things so it would be the costs of the developers of the EHRs. Additional cost savings would be realized by users who wouldn't have to sit on the fence and delay implementations while they had the vendors or the vendor and the HIE or whoever the other source is, sort out the kind of problems that we discovered in the dealer VLER testing. I don't know any rational way to calculate that, but I think it's several times larger than the savings simply in programming costs Obviously money that's saved for users and vendors doesn't generate money in the federal government, it doesn't work that way, but the ability of the government to fund what I think is a much less expensive capability than \$75 million, the fact that it can generate this savings is a rationale for doing it. Thanks for listening.

John Halamka – Harvard Medical School – Chief Information Officer

Great. Thanks very much, Wes. Others who would like to make comments on this consolidated CDA topic?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

David.

John Halamka – Harvard Medical School – Chief Information Officer

Please go ahead.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I have to question, last time, and I just want to register it again maybe for Doug, is it seems to me that CDA is still somewhat of a moving target and I'm wondering how the consolidation through a moving target will be handled. Are you going to freeze a current definition of CDA structures and then revisit them if we should move more aggressively toward greenCDA, or if the detailed clinical model works its way into changing the way we encode deeper clinical structures in XML. How do you deal with the moving target that is CDA?

Doug Fridsma – ONC – Director, Office of Standards & Interoperability

I think you raise an important point, and it's one of the reasons why we've also tried to think ahead to what would be necessary if we were to improve the ways in which the standard is represented and the implementation specifications, that simplification still will require some tools or some mapping and some education. I think there's two things. One thing that you raise is this notion of greenCDA, and just at a very high level, and I think Wes talked about this with this notion of XPATHs, you can imagine that a particular section is identified by saying template ID equals and then a large number occurs after that, or you could say medication list, and greenCDA is really trying to get closer to the latter, which is medication list rather than template ID equals this large number. The challenge is within the greenCDA work is that it

is a moving target and somebody might say medication list and someone might say past medications and someone else might say current medications, and that difference between using those labels on there, makes it harder for computers to be able to understand. They may be looking for medication lists and what they see is past medications and computers don't know necessarily how to resolve that.

One of the things that has to happen as we move towards this is to get pinned down what those individual templates would look like. So there is discussion that's going on within HL7 to bring those forward and have a community take a look at them to ballot them and to be able to say this is the way that that particular template needs to be represented. That work isn't done, but once that happens it becomes much easier because it stops being quite such a moving target. It probably is going to take us a number of months to work through that process with HL7 and the standards development community. In the meantime, I think it's important that we have mechanisms to be able to map between the current way of doing things and this more consolidated CDA approach. And so we are working on some of those activities. We want to make sure that people can make the translations back and forth as need be. So I think in the short term mapping will help us. In the short to medium term getting standardization around what those building blocks look like will make it much, much easier for the vendors to know what the target is. Even if you could assemble those different building blocks knowing that there's 38 building blocks to work from and these are how they should be represented I think is very helpful.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

John, can I comment on one point?

John Halamka – Harvard Medical School – Chief Information Officer

Please, go ahead.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Doug raised the issue of business names versus XPATHs, and he pointed out that it can be very helpful to say medication list to the programmer who's trying to figure out what this particular flavor act in what mood refers to medications and lists thereof, but it's not helpful in the wire standard because it has to be interpreted by computer. My understanding, which is secondhand, is that the consolidated CDA was revised in the last iteration to include business names. That's helpful for the programmers, as we described, but it also seems like the basis for standard business names. So if the standard business name is medication list in greenCDA instead of an XPATH, which is a lot longer than just a template ID, it specifically includes multiple XML element names and attribute codes in order to identify a specific data element, if HL7 has already made a lot of progress in establishing standard business names it's a natural next step to establish standard greenCDA based on the standard business names.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

This is David. I'll just piggyback on that and say an oid is the standard business name that humans can't read. You might as well have standard business names that humans can read.

John Halamka – Harvard Medical School – Chief Information Officer

That's a very good point. Others who would comment on the consolidated CDA topic?

Arien Malec – RelayHealth – VP, Product Management

This is Arien.

John Halamka – Harvard Medical School – Chief Information Officer

Please, Arien, welcome.

Arien Malec – RelayHealth – VP, Product Management

Thank you. Just two responses to Wes' I think really excellent list of suggestions for NIST. One is a preference for depth search testing as opposed to ... testing. That is to say, it's better to test all the way through to deep semantics on a medication list than it is to cover every possible section in the consolidated CDA.

The second is perhaps some notion of randomizing, within a larger set, the list of semantics or the list of coded terms. That is, it's really easy to gain the system if you know, as Wes noted, that not only do you not get interoperability ... to gain the system if you know that the test script will always test medication X versus medication Y, and having some 95% sub-lists, as I think we've discussed in the past, that you then pull codes from for testing would be very useful.

The last point, and I'm somewhat embarrassed to say that I don't know the current status of this, is that in the transition in care work the folks were defining expectations for clinical semantics for things like medication lists, that is, defining that it be an active medication list and then defining what to do if, for example, on referral and consult note back the medication list had been changed, the clinical expectations, and then the associated CDA coding expectations. Those kinds of things, those kinds of business rules or interpretation semantics on top of CDA would be really useful for deeper interoperability.

John Halamka – Harvard Medical School – Chief Information Officer

Great. Thank you for that comment. Any other comments on the CDA topic?

Tim Cromwell – VHA – Director of Standards & Interoperability

Yes, this is Tim Cromwell.

John Halamka – Harvard Medical School – Chief Information Officer

Please, Tim, go ahead.

Tim Cromwell – VHA – Director of Standards & Interoperability

Thank you. Wes' comments were very eloquent and extremely accurate. I don't know who in the hallway Wes has been talking to, but I can imagine that it's from a small team of folks that we've had working on the results of the interoperability projects in VLER for quite a while. We've come to understand, and this is really where a really good, solid understanding of this notion of standards disparity or the standards not being able to implement C32 out of the box has come from, so when we talk about consolidated CDA and the next level that we need to get to, it's extremely important, and I agree with it completely. What I'm worried about is that I'm more convinced than ever that a year from now we're going to have 50-60 eligible exchange partners with VA through the VLER project, whole states who are now in the on boarding process and they're making the decisions, those technology partners and state HIEs are making the decisions right now about what specifications they're working on to develop the CDA or the C32 for interoperability and for exchange with us.

And so if we can take advantage of the opportunity that's in front of us right now and escalate it a bit, I think we can help those exchange partners and their technology partners to make the right decisions so that six months or a year from now when we are reaching out to them and doing point-to-point what we call partner testing, that we are not going to have to have 60 different efforts to do partner testing, that instead we'll be able to bring these folks on and do interoperability more quickly. And that will be more consistent with their desires and it will certainly enhance our VLER program quickly. So what I'm advocating is if we can look at the consolidated CDA project and enhance that and accelerate it in any way, VA would be very much in support of that.

John Halamka – Harvard Medical School – Chief Information Officer

So let me just summarize all of our CDA discussion. Doug, I think we've heard from Wes, we've heard from Tim, and we've heard from others in the industry that you are solving a very important problem, move fast, because one wonders if we are going to be using the CCD C32 increasingly and there are different implementations guides written like the New York and multi-state collaborative to try to constrain it, and at the same time you are fixing a lot of the problems and we've run the risk of having less interoperability in the short term than we'd like. And this is of course Steve Posnack's question here we have a set of work in flight that looks very promising how do we appropriately balance the newness of this work and the notion that you have a time constraint, so more to come.

On all the topics of the S&I framework I think, Doug, we want to at our next meeting in November continue to drill down on the consolidated CDA and its acceleration, but also we've raised these questions that would be useful to discuss with ONC and at our next meeting of how we take additional testimony on NwHIN exchange and how we as a standards committee can help look at some of the areas of NwHIN exchange that need some enhancement and even consider how a workgroup might be formed to talk about RESTful approaches, then again also at our next meeting how do we organize ourselves to begin talking about radiology test results and image exchange. I think, Doug, since you're always so influential in your role of helping us form our agendas, probably with Mary Jo we can work on getting those into our agenda for next meeting.

Doug Fridsma – ONC – Director, Office of Standards & Interoperability

Thanks, John. I think one of the things that we may think about, and I'll throw it out there with the group, I know that we've got a face-to-face meeting that's coming up in November and I think in December we're anticipating a virtual meeting, I think it would be useful for us to find a way to have a public felicitation for written descriptions or written testimony and then maybe we can then summarize that or provide that to the committee for their review. That may be the most expeditious and cost effective way to move forward than to try to plan between now and the end of December a face-to-face hearing, if you will. We might be able to provide broader input in a more timely way.

John Halamka – Harvard Medical School – Chief Information Officer

That sounds very useful.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

John?

John Halamka – Harvard Medical School – Chief Information Officer

Yes?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

You make *Reader's Digest* look like ... in terms of finding the right words to summarize a complex thing and do a great job. However, I did want to be sure that at a fairly high level in summarizing our work we included the point that we're suggesting, online testing tools and a best practices council to deal with issues as they come up for future consideration.

John Halamka – Harvard Medical School – Chief Information Officer

Absolutely, we want to capture that idea.

Tim Cromwell – VHA – Director of Standards & Interoperability

This is Tim. I strongly support both of those items as well.

Doug Fridsma – ONC – Director, Office of Standards & Interoperability

And let me just mention as well at some point, and I don't know what the right form is, but at some point it may be useful to provide to the committee or in some other venue, if that's more appropriate, a demonstration of some of the existing tools that have been developed, certainly to get some input on those and the functionalities that are in some of those tools might be very helpful, and see whether those are on track with where people are thinking we need to go, or whether we need to make some course corrections to see. We can take a look at NIST tools. We can take a look at some of the MDHT tools that we've got to help develop the specifications, and I'd be happy to, again, maybe brainstorm about how best to do that, whether we want to do a Webinar or if we want to have a meeting of a subcommittee to do that, synthesize it, and present it back to the committee.

John Halamka – Harvard Medical School – Chief Information Officer

Very good. So as we ... that next agenda for November I think that we should carry forward with this topic of looking at the tools, advancing the greenCDA initiative, and trying to make implementation simpler for everyone.

We'd like to move on now to the Steve Posnack discussion. As I introduced the meeting and I described Steve, a notion that we need to tell the vendor community how they send a transaction from point A to point B. Do they include an envelope around every payload before they put it into a direct format? What is the use of these CDA R2 standards that we've worked hard to specify? So we look forward to hearing your comments on how the industry has reacted to them.

Steve Posnack – ONC – Policy Analyst

Thanks a lot, so twice in one day for me already. I'm going to be running through, and I'll make sure I say next slide so that folks that are driving for me can follow along. As John alluded to, we, and I should probably go to the next slide right now, I'm just here to give folks an update on the advanced notice of proposed rulemaking that we published in the federal register in August. The ... closed a little bit less than a month ago. We had introduced the concept of the three categories of metadata that the power team had presented to the Standards Committee, and we included a number of questions, 20 questions to be exact, that we were soliciting specific input on. We received a little bit over 50 comments from the industry at large, and I'll go through how folks broke down and some rough categorizations. As a quick note, this is a reflection actually of how we've been able to distill the comments down thus far and to give folks an update that it's not meant to represent our ONC opinions or positions that we have. Next slide, please.

I'm not going to dwell on this too long. This is just to give folks a breakdown, rough categories of the type of commenters that we had. Next slide.

In terms of some general analysis, folks were largely supportive of the use of metadata generally and the benefits of metadata. Some were opposed to having federal regulations specify what they should be and that the standards development organization should go out there further. We had asked a specific question whether or not metadata standards would be ready to include in Stage 2 Meaningful Use oriented requirements and nine specifically noted that they didn't believe that the industry is ready. It's hard to tell sometimes unless there's an explicit response of a no, we don't believe this is necessary, whether folks are on the fence, have a general distaste for the Stage 2, were ambivalent is unclear sometimes, so we did have a firm nine that we could identify as no's. In terms of using the CDA R2 header, some folks reported it, of the 11 no's out of the 27 folks just didn't think we should specify the ... as the standard as part of the regulations and only specify the metadata elements that needed to be associated. Next slide.

Like I mentioned, we posed 20 questions and they broke down based on the categories underneath each category, so patient identity, provenance, privacy, which included the policy ... and the categorizations. We also asked implementation considerations for the use cases that we had included and any other additional considerations, standards, and metadata representation structure. Next slide, please.

I'll probably just call out a couple of things on each of these since they are fairly detailed, and if you got a chance to read through them in advance of today then you probably have already seen a majority of what I said. I promised Kevin I wouldn't read through all the slides verbatim, so I'll definitely try not to do that.

We had specified a few default things, for lack of a better word, that would be part of patient identity metadata that would also conform with the CDA R2 as it stands, and we got a lot of interesting feedback in all three of the categories for the questions that we asked, or related to the questions that we asked. A lot had to do with the, and I don't know if there's a standard term for this, but how current the data was that could be represented, so both with name and with ... and with address – sorry, with name and address mostly folks identified that the date ranges associated with them would be important to have as well. We got a number of folks that had identified additional patient identity elements, and those are on the next slide, and pretty close to going down in order of the number of commenters, gender was one that got identified for inclusion in terms of additional patient identifiers, place of birth, mother's maiden name, and then other specific ones that the patient matching team has also identified in their past work. Next slide, please.

For additional consideration commenters suggested that certain elements should be considered for removal because they didn't see particularly tremendous value in including them. A majority, and those are listed there, a majority of commenters believe that if the individual lacks the direct information then it would not be appropriate to include the institution of the direct. This is something that came out of the poll comments that were received, and I don't recall that we had asked a specific question relative to this, but the trend in response was so high that we thought it would be good to include it in the slide deck. Next slide, please.

This is on to provenance. A good majority of the 21 that commented on additional provenance elements identified other specific data points, like the dates of service, the actors and their credentials, the types of service performed. We also had asked a question about the relationship to the digital signatures and whether that should be part of metadata and the element that would be included in the digital certificate, and should that be wrapped as part of S/MIME or it should be part of just the general metadata that are attributed to a document, for example. A majority of folks suggested that the time stamp actor and actor's affiliation needs to be expressed in the XML syntax specifically rather than including it separately as part of a digital certificate. So that was one of the questions that we had asked, I believe, and it seems like the commenters are pointing to a specific direction. Next slide, please.

The comments on the privacy, as was evident at the Standards Committee when these recommendations were presented, generated a lot of feedback, one of which suggested that metadata should only describe the data set, that there should be a separate layer, and I think this falls under the construct that's in the HITSP transaction package 30, which is the managing consent directive transaction package. Also, which I think is identified at the Standards Committee when this was last picked up, commenters had concerns about how the ... could lead to inferences and inadvertently divulge sensitive information. Next slide, please.

We asked questions about the policy pointers that were recommended as part of the metadata. A number had identified that they would be problematic and also recommended that they shouldn't be part of Stage 2 certification, and here are some of the reasons why folks suggested that we exclude policy

pointers in metadata at the present time. Policy persistence, which I believe we touched on in the preamble of the ANPRM and we asked for comments on, was one of the primary reasons why folks didn't think that this should belong as part of the metadata at the present time, also that the privacy policy couldn't be expressed in a computable fashion. Next slide, please.

There's a lot of discussion about the "sensitivity" and how that's expressed in metadata. We asked a specific comment about the confidentiality by info type versus the confidentiality by access kind, which is our data sets or value that are expressed in HL7, and we got a lot of feedback that confidentiality by access kind, I guess value set or code set, should be looked to versus the confidentiality by info type, which I believe was part of the either metadata ... suggestions or was discussed as the initial set of sensitivities that could be used to use it as part of the metadata vocabulary. Next slide.

In terms of the overall metadata representation and structure, folks generally supported the use of the CDA R2 and its header. Some were concerned about the changes that we proposed based on the metadata power team and the Standards Committee's recommendations to the CDA R2 header that would be non-compatible. Just to give folks a reminder about some of the tweaks that were suggested, one was using the uniform resource identifier, URI, to act as an ..., as opposed to the object identifier oids that are currently specified in the HL7 CDA R2. Several commenters asked that we, again, only specify the metadata elements and not the representation structure, and others identified that we should look at XDS instead of the HL7 CDA R2. Next slide, please.

The implementation series and use cases, we were particularly interested, and we asked a specific question about how heavy of a list it would be for developers to include metadata assignment capabilities to particularly use cases, and the use case that we had identified, and for those of you that were part of the interdisciplinary team on the Policy Committee side that first looked at the PCAST Report and reactions to where ONC could go, one of the initial use cases that was identified had to do with attaching metadata when a summary record would be provided to a patient or sent to their personal health record or other type of third party. And that seemed to be a first step and first type of capability that could be included in EHR technology as part of certification. Some believe that EHR technology was mature enough to include this type of capability; others felt that not enough progress had been made and that additional analysis and additional testing was needed. Other potential use cases, since we had requested public comment I wanted to say if you didn't think that this could be such a heavy list, what other use cases could benefit from the assignment of metadata and some of those are the ones that we ... below. Next slide, which is my final slide here.

Most commenters identified that of the metadata categories we had proposed for the duration patient ID provenance and privacy were generally a good small set of metadata categories. Most felt that the standards to support privacy metadata, as I had mentioned before, still were in an immature state and needed some additional work, probably at the SDO level. Several commenters pointed out that the metadata elements that could be used for patient ID provenance and privacy weren't mutually exclusive and had raised some points relative to having the metadata categories be better described and how those metadata should be viewed, and then some commenters recommended that ONC clearly define expectations or requirements for managing changes to certain metadata elements, which obviously is another struggle and challenge for things that change over time.

That concludes my quick and dirty run through of the comments that we've been able to distill from the 50 or so that we got in response to the ANPRM. I did want to take a brief moment to thank the two members on my team, Jamie Skipper and Jennifer Frasier, that have been combing through all the comments that were received in the past three weeks and in preparing the slide deck and the data analysis that quantify

the types of feedback that we receive. I'm not necessarily sure I can answer a specific question, but I'm happy to take any. You all are obviously free to have a quick discussion if you feel it necessary. Thanks.

John Halamka – Harvard Medical School – Chief Information Officer

Great. Well, thanks so much for all the hard work. Assembling these comments into themes is always really quite tough. Let me open it up to the committee, specific questions or comments in response to what Steve has presented.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

This is David, I have one.

John Halamka – Harvard Medical School – Chief Information Officer

Go ahead.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think in looking at the NPRM it was a little bit unclear to some of us who discussed it as to exactly what problem was trying to be solved with the metadata. And in terms of going forward, it might be helpful to focus on a specific small set of problems and look at it as an experiment or a pilot, instead of imposing it on a broad swath of state interchange. The one that concerns me that I think we as a group would like to encourage, but which if you don't have some kind of metadata could be problematic is when data leaves the control of an EHR or an HIE and passes it to the consumer, the consumer patient, and then that consumer takes that medical data and introduces it into another system that has no contractual or control relationship with the originating system, that specific use case, which I think we'd all like to encourage, is the one that seems to me benefits especially well from some kind of assurance that the data hasn't been tampered with in between the originating system and the unknown future receiving system. So I would just put that out as a use case to drill in on if you are considering regulating around this when you're moving data between two control systems but in the hands of an uncontrolled transport vector, namely the patient.

John Halamka – Harvard Medical School – Chief Information Officer

Well said. Now, in terms of the problem to be solved, I think this whole thing came out of PCAST originally but the notion that we have multiple payloads, X12, NCPDP, HL7, consolidated CDA, and wouldn't it be wonderful as we transport this from place to place in a consistent envelope and it enables us to figure out where it came from and who it refers to, as opposed to having to dive into the payload itself. I think everyone agrees that this sounds interesting but pilots absolutely are required before going forward with it broadly.

Other comments people would make?

Stan Huff – Intermountain Healthcare – Chief Medical Informatics Officer

John, this is Stan.

John Halamka – Harvard Medical School – Chief Information Officer

Go ahead.

Stan Huff – Intermountain Healthcare – Chief Medical Informatics Officer

I'd just really like to second what Dave said. You would have a lot to understand, he characterized them as problems, I would characterize maybe as use cases, to think the situations in which we're trying to use this, you can imagine at a high level that it could be the target of this and the use cases around division of ... and a much more fluid information exchange, or that this could be applied to more traditional HL7 style or DICOM style data exchange. And even if you said this was restricted to PCAST, I don't know of any

authoritative document that describes the information flow and that would allow you to take these specifications and say, oh, in this information flow there was an initial query for data that was sent from party A to party B and the query was answered against a database and came back to the requesting party, and that's the message that this metadata is in. Plus, the context also that was probably very important about whether this was a query about an individual patient or this is in fact a public health query and what you're going to get back is a collection of data about a series of patients who answered the query, it seems to me that this whole discussion would be helped immensely by specifying the use cases we're trying to cover. And it doesn't have to be one, but I think we have to be explicit about them, or we don't know whether what we're proposing is in fact good for use. So I strongly second Dave McCallie's call to just have some more public and explicit discussion about what the use cases are that we're trying to meet and the information flows that we would support using this metadata.

John Halamka – Harvard Medical School – Chief Information Officer

Great, thank you. Other comments? Well, it appears this must not be too controversial a topic. Steve Posnack, is the notion of the next step on this, you heard some important feedback about the need to describe, what are we trying to accomplish? Is there going to be an NPRM that follows that would presumably then incorporate some of the recommendations you've heard from us and from commenters?

Steve Posnack – ONC – Policy Analyst

Yes. I think, as we alluded in the ANPRM that proposed all these questions, our intent would be to process all of the feedback, which we're still in the process of doing, from all 50 commenters and see where there is a place to include a proposal in our next rulemaking the NPRM for the standards and certification criteria that both Liz and Judy's group had recommended, and Dixie's today, as part of the bigger package for the next round of certification. That's the process that we're currently under, investigating where there might be something that we could pursue, and taking into account the commentary today as well as the feedback that we received thus far.

John Halamka – Harvard Medical School – Chief Information Officer

Very good. Well, Doug and I have been exchanging some messages, and just as some follow ons to this entire meeting today Doug will speak with ONC staff, Mary Jo and others, to think about the best way to seek written testimony analytic exchange experience. We will craft an agenda for our next meeting that does follow on the S&I framework discussion, and we'll demonstrate some of the tools that are being created that address some of the concerns that Wes and others raised. So we should have very good momentum as we continue our next body of work.

Steve, important question before we move on to public comments, have we delivered to you, in a timely way, everything you need to now move forward with your regulation writing?

Steve Posnack – ONC – Policy Analyst

I believe the answer is yes, and I thank everybody for devoting a lot of time over the past three months to really react to the Policy Committee's recommendations and putting in a lot of good thoughts.

John Halamka – Harvard Medical School – Chief Information Officer

Wonderful. Well, we aim to please. So thanks very much, everybody on the Standards Committee. I certainly second Steve's comments that we celebrated in the White House in September, today we've added some additional polish and comments and importantly delivered the next privacy and security certification guidance, so Steve should be in good shape, on time.

Let me turn it back now to Mary Jo because I believe you want public comment.

Mary Jo Deering – ONC – Senior Policy Advisor

That's correct, John. Thank you very much. Operator, would you open the lines and see if there's anyone who would like to make a public comment and give them their instructions?

Operator

(Instructions given.)

John Halamka – Harvard Medical School – Chief Information Officer

Do we have any commenters?

Operator

We do not have any comments at this time.

John Halamka – Harvard Medical School – Chief Information Officer

Okay, very good. Well, folks, thanks again for all of your ideas and participation today. We will certainly be in touch as we craft the agenda for our next meeting. I look forward to seeing you in Washington in November. Mary Jo, unless there's anything else, I think the meeting has adjourned.

Mary Jo Deering – ONC – Senior Policy Advisor

I don't believe so. Thank you, John.

John Halamka – Harvard Medical School – Chief Information Officer

Thank you. Have a good day.