

**HIT Standards Committee  
Privacy & Security Workgroup  
Transcript  
March 20, 2013**

**Presentation**

**MacKenzie Robertson – Office of the National Coordinator**

Thank you. Good morning everybody. This is MacKenzie Robertson in the Office of the National Coordinator for Health IT. This is a meeting of the HIT Standards Committee's Privacy & Security Workgroup. This is a public call and there is time for public comment built into the agenda. The call is also being recorded so please make sure you identify yourself when speaking. And just as a matter of process for this call, since there was so much interest in the presentation being given on data segmentation, we do have two other workgroups of the HIT Policy and HIT Standards Committee listening in. The Privacy & Security Tiger Team and the Clinical Operations Workgroup are also listening in to the call. I'll just ask that those two workgroups, the Tiger Team and the Clinical Operations Workgroup, if you could please hold all your questions until Dixie makes an announcement for additional questions after the presentation, to allow the Privacy & Security Workgroup questions to go first. And I'll now take role for the Privacy & Security Workgroup. Dixie Baker?

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

I'm here.

**MacKenzie Robertson – Office of the National Coordinator**

Thanks Dixie. Walter Suarez? John Blair? Mike Davis? Mike, are you on? I believe Mike Davis is on. Tonya Dorsey?

**Tonya Dorsey – Blue Cross Blue Shield, South Carolina – Chief Implementation Architect**

I'm here.

**MacKenzie Robertson – Office of the National Coordinator**

Thanks Tonya. Lisa Gallagher? Leslie Kelly Hall?

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

Here.

**MacKenzie Robertson – Office of the National Coordinator**

Thanks Leslie. Chad Hirsch? Peter Kaufman? Ed Larsen? David McCallie?

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

Here.

**MacKenzie Robertson – Office of the National Coordinator**

Thanks David. John Moehrke? Sharon Terry?

**Sharon Terry, MA – Genetic Alliance – President and Chief Executive Officer**

Here.

**MacKenzie Robertson – Office of the National Coordinator**

Thanks Sharon. And any ONC staff members on the line, if you could please identify yourselves?

**Will Phelps – Office of the National Coordinator**

Hi MacKenzie, Will Phelps.

**MacKenzie Robertson – Office of the National Coordinator**

Thanks Will.

**Melissa Springer Melissa Springer – Office of the National Coordinator**

Melissa Springer.

**MacKenzie Robertson – Office of the National Coordinator**

Okay. And do we have Joy Pritts on the line?

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

This is Stan Huff; I'm also on the line.

**MacKenzie Robertson – Office of the National Coordinator**

Thanks Stan. Will, can you just ping Joy?

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

I notice Walt – I thought I had heard Walter earlier, but I think it's important that Walter and Joy be on the line.

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

Yes, hi Dixie. Good morning, this is Walter.

**MacKenzie Robertson – Office of the National Coordinator**

Thanks Walter.

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

And, Dixie, Jaime Ferguson is with me here, too.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Okay. Well you may not have heard, you might want to repeat the logistics there, MacKenzie, for those who joined a little late.

**MacKenzie Robertson – Office of the National Coordinator**

Okay, just so everyone is aware, this is a Privacy & Security Workgroup call, but since there was so much interest in the data segmentation presentation that's going to be heard today, we did invite two additional workgroups of the HIT FACA committees. We have the Privacy & Security Tiger Team, some of the members on the line, as well as the Clinical Operations Workgroup. But I'll just ask that those two additional workgroups just hold your questions until Dixie makes an open announcement at the end of the presentation for you guys specifically to ask, so we can just triage the Privacy & Security Workgroup questions first. So with that, Joy, have you joined yet? No, okay. So Dixie, I'll turn the agenda over to you and then I'll email Joy separately.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

All right. Thank you. I'm sure Will will try to track her down as well. I want to welcome everybody, all 3 workgroups to this call. I know that certainly the Privacy & Security Workgroup has been really looking forward to hearing about some work that Joy Pritts' team there in the Office of the Chief Privacy Officer, has been doing on data segmentation. You may – I'm sure that you recall that the HITECH Act included a specific request in it that the Office of the National Coordinator investigate technologies to address the segmentation of data, where segmentation was defined as, either directly or indirectly, as those kinds of data that require special protection under the law, such as substance abuse and sexually transmitted diseases, etcetera. So, we're really looking forward to hearing this report back from that team. I had also asked, or maybe just tell the Privacy & Security Workgroup, at the last Standards Committee meeting, the ONC went over a number of tasks for our consideration and that they would like to have done in 2013. And one of those tasks did have to do with data segmentation. So, this will provide some input into that task as well.

And finally I want to welcome the other two, the Clinical Operations Workgroup members and the Privacy & Security Tiger Team members to this call. And as MacKenzie said, we'll hold the questions from those two groups until the end, before we have public comment. Okay, with that, let me turn it over to Will. Maybe you can introduce the people that will be presenting today.

**Will Phelps – Office of the National Coordinator**

Good morning everyone. This is Will Phelps, ONC. Today Johnathan Coleman, who has worked with the Data Segmentation Project for Privacy, that ONC's been working on, will give the presentation on data segmentation. Joy, the Chief Privacy Officer, will give a brief introduction on the initiative, before Johnathan presents.

**MacKenzie Robertson – Office of the National Coordinator**

Joy has joined, too.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Good.

**Joy Pritts, JD – Office of the National Coordinator**

Yeah, sorry about that. I got kicked off when they put me into the public line. I thought – I took it personally at first, but I dialed back in.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Good.

**Joy Pritts, JD – Office of the National Coordinator**

Okay. Well, good morning everyone. It's our pleasure to be here and to share with you some of the progress that's been made on the data segmentation initiative. As you know, this Initiative was launched a little over a year ago, in response not only to, as Dixie was mentioning, the HITECH mandate, but also some of the recommendations that we've received in from the Policy and Standards Committee, as well as the National Committee on Vital Statistics. In addition to our federal advisory committees, we also received some input from the President's Council of Advisors and Science and Technology, with respect to tagging data for use and in order to enable people to indicate some of their choices, and to have those choices implemented in an electronic environment.

This is a, I think, a very important project going forward, because we have heard from the field that right now, a lot of health information exchange is excluding behavioral health providers because they...the people who are engaging in this kind of exchange don't know how to technically handle the information, with its additional restrictions on it. And so we are delighted that we think that we have made some progress in this area that will be very useful for people. There have been a – I'd like to thank everybody who has participated in this project, particularly Johnathan, who has so widely led this project and in a very calm manner, even when there was a lot of tension over a lot of different issues.

We've had close to 150 participants in this project and as Jonathan will describe to you in a few minutes, we have five announced pilots, four of which are from the private sector. So we are very excited about where this project is headed. So I will, without further ado, turn this over to Johnathan, with great thanks.

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

Well thank you very much Joy and also thank you to Dixie and Walter and members of the Committee for allowing us to present today. And I do believe that Ioana Singureanu is on the call as well, and Ioana has been instrumental in helping us and the community develop the technical concepts. So, Ioana will be co-presenting with me and will be able to assist with any standards specific related questions that may arise. So with that, I just want to thank you all and my role here is Initiative Coordinator, very fortunate, I get to be the messenger. So please understand that the work that we're presenting today really is the work of the community and hundreds of hours and many, many minds far smarter than mine have gone into developing our work products and helping architect the solution. So, I'm very privileged to be able to present a synopsis of the work that was done throughout the community, within the Data Segmentation for Privacy Initiative, over the course of the last 12-plus months. I think we can go into the main presentation materials please.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Jonathan, just, for those of you who may, especially those on the West Coast, be sure to check your mail because we did receive a copy of this presentation this morning.

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

Thank you Dixie. Okay, so this begins our report. I think we can advance to the next slide please. So, our presentation agenda for today, we have quite a lot of material to get through and I know some of you have seen some of these slides before, so I will go fairly quickly through the first few slides, where we remind folks and introduce data segmentation for those who aren't particularly familiar with it, about our approach. So, that would include the purpose and need for data segmentation for privacy, some of the technical challenges that we've been facing and then we'll dive a little bit deeper into our technical approach, explain some of the building blocks and walk through the selected standards. We'll then switch gear a little bit and talk about the actual work products that have come out of the Data Segmentation for Privacy Initiative, which was an initiative of the Standards & Interoperability Framework. And then we'll wrap up with our conclusions.

Next slide please. Okay, so let's begin then with the purpose and need for data segmentation for privacy. So, a little bit of background here. Some healthcare information requires special handling that goes above and beyond the protections that are already provided through the HIPAA privacy rule, which, as you know, allows healthcare providers to disclose protected health information, without patient consent, for the purposes of treatment, payment and health care operations. And protection through the use of data segmentation emerged in part through state and federal privacy laws, which addressed social hostility and stigma associated with certain medical conditions. And there was a SAMHSA paper dated from back in June 2004, which contains a lot of the research and substance behind that last bullet and so I would encourage people to have a look at that paper, which was really a good source of information as to why data segmentation is needed.

Next slide please. So here are some examples of heightened legal privacy protections in the US realm, and there are others, but just introducing the first 3, which are the ones that we really focused on during the data segmentation and privacy initiative. And the first of those is 42 CFR Part 2, often just referred to as Part 2, and that's the Federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations, which are designed to protect specific health information from exchange without patient consent. Title 38 is a law that protects certain types of health data that comes from covered Department of Veterans Affairs facilities and programs. And the types of data there include sickle cell anemia, HIV, as well as the substance abuse information. And that rule...that title is very closely modeled on the 42 CFR Part 2 requirements. And then finally on this slide, we have the new rule, which became effective, or which becomes effective March 26, and in this final rule, it describes how patients may withhold any health information from their health plans for services that they've received and paid for out of pocket. But, this is a new rule and please note that it's the patient and not the provider, who has the responsibility for ensuring that downstream recipients know that the patient is requesting that restriction. So, these are the three rules that we looked at when we were developing the use case document within the Initiative, and so, a little bit more to come on that later on.

Next slide please. So while we did focus on those three requirements that we just described – so just back one slide – it's important to note that the principles and the design that the community developed throughout the initiative was designed to be extensible, so a broader range of privacy policies than just the three that we described. So, for example, there are state and federal laws that also exist to protect data related to certain conditions or certain types of data, such as data regarding minors, genetic information, intimate partner violence and sexual violence and HIV related information. So while our solution focused on two well-known privacy laws, and then the third one, which is fairly new, again it's important to note that we did expect this solution to be extensible to a variety of different privacy policies.

Okay, next slide please. All right, so let's look at some of the technical challenges, and we captured a couple on the slide that's coming up, and please note also that there were plenty of policy challenges as well, but we did focus on the technical challenges – the technical challenges were the focus of our workgroup. And while the policy debate was certainly very interesting, it wasn't our charter to try and solve the policy challenges that were placed before us. So we did concentrate on the technical challenges and on the next slide please, we have some of those technical challenges listed. So in general, there was much discussion on the technical side about how to segment data. So there are multiple levels at which segmentation can occur, for example, the disclosing provider, perhaps the intended recipient or the category of data such as medications. And we've found that technically there were no widely adopted standards available or in use to segment at those levels or for transferring the restrictions that may be placed on that data across organizational boundaries, for example, for redisclosures.

Additionally, unstructured data. So the prevalence of free text does complicate the identification of the information that is subject to this enhanced protection, and then we also stand that granularity is a concern. In the current implementations that we really heard from our community about, there was a reliance on out-of-band handling, because the ease of implementation technically for opt-in or opt-out is easier to implement than a more granular choice. So, definitely the more granularity you add, the more complex the solution.

All right, the next slide please. Let's go into our technical approach now. And what we've tried to do in the next few slides is really simplify and try to explain in a way, how we developed building blocks and using these building blocks to accomplish the data segmentation for privacy solution. Next slide please. So, we have this "Russian doll" concept of applying metadata with decreasing specificity as layers are added to the clinical data. So in other words, the most revealing information is at the heart of the transaction, within the clinical payload, and as you get further away from those clinical facts, and by applying metadata or additional layers, we have data and metadata that is less revealing with each additional layer, okay. And we expand this to convey the confidentiality of the data within the clinical payload, so that is a security label. Obligations of the receiving system, so for example, any dissemination or special handling instructions and then finally the allowed purpose of use, so the reason for the disclosure in the first place. And these three key areas are really our three primary building blocks.

Next slide please. So let's look at these in a little bit more detail. So with confidentiality codes, the need for the security levels, these may be used by systems to help convey or enforce rules regarding access to the data that requires enhanced protection. And we use the highest watermark approach here. So in the little bracket that you can see on the slide, this is just a fairly clear representation of a CDA document with different sections. And you can see in this particular example, we're applying confidentiality codes of restricted to two of the sections, but not the third, but the highest watermark approach applies. And so the overall document confidentiality level of restricted, essentially floats up to the document header, and please note that this is intended to be a capability of the data segmentation for privacy solution that receiving systems may use to be able to identify data at the section level that requires enhanced protection. But if receiving systems don't have that capability, they can use the restriction at the document header level to interpret all of the data within that same document as having the same labels. So, we do expect this approach to be backwards compatible with less sophisticated systems.

So, moving on to the purpose of use. As I mentioned earlier, this defines the allowed purposes for the disclosure, and we primarily dealt with treatments and emergency treatment. I'd like to add that one of the user stories that we have developed in our use case document deals with emergency access to clinical data in a break-glass situation. And then the third building block, the obligations. So these are refrain codes and obligation codes, but the refrain codes are specific to those obligations being placed on the receiving system, for example, do not re-disclose without consent. Okay, next slide please. So ...

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Johnathan, do you mind if we ask questions as you go or should we wait until the end.

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

No, I think it would be great to have questions as we go. And we do have quite a few slides to get through, so if it's okay, we will take questions on the way, but if it looks like it's going to be a long debate, then perhaps we can table them until the end.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Okay, or – all right, then let me ask a question about that last slide. You said if the EHR system is incapable of handling the sectioned metadata, can't interpret the metadata that are on the sections, that it defaults to the overall CCD label?

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

Yes, that's correct.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Right. Does the sender ever know that or is there a way that the senders can even find out what they can handle?

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

Yeah, so, within our use...that's a great question Dixie, thank you. So, within our use case document, and in the implementation guides, we do have prerequisites in there and among those prerequisites are that there is a trust agreement between the exchanging parties. And there would be an expectation that the sending party would have an understanding of what the receiving party was capable of doing technically. But the idea here is that having vague details, section level restrictions would aid the receiving system in being able to make access control decisions by tagging that data at the most granular level that they are capable of. But if they're incapable of making active control decisions within the section of the CDA, they have the ability to default to the overall restriction that was placed on the document, and that's why the highest watermark approach applies, because it has a more privacy aware approach than the less revealing method.

**Ioana Singureanu, MS – Eversolve LLC**

And Johnathan, if I may add, from a conformance standpoint, those criteria that must be implemented by everyone are identified as shall and those that may or should be implemented have a lower degree of conformance. So, it should be very clear from the implementation guide that the specification of the confidentiality of document level has to be observed by the receiver. So the sender would know also from that context, which capabilities may be implemented by a receiver or shall be definitely implemented by a receiver.

**Clement J. McDonald, MD – National Library of Medicine**

This is Clem McDonald. This assumes, I gather, that the only way one can send any information is CDA, which cuts out something on the order of 60 billion HL-7 messages being sent a year now.

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

I think that what we were trying to do here is be payload-agnostic. We did focus on the Consolidated CDA as the primary clinical payload for meaningful use purposes. But, our solution does allow non-CDA documents also, obviously not within the section level or entry level, but Ioana, could you elaborate on that a little bit please, about ...

**Ioana Singureanu, MS – Eversolve LLC**

Sure, sure. So, yeah, the example in front of us is a CDA document, but the privacy metadata applied at the transport level would apply to anything, so, as Johnathan mentioned, this level of privacy metadata annotation applies at different layers. So you're looking inside the most nested Russian doll right now that could be something other than CDA. But, there could be privacy metadata applied at the transport level, so if you're exchanging a PDF, or an HL-7 version 2 message, you would have a place for this metadata to live, and again, be less precise as far as the reason for why the data is sensitive, and be specified at the transport level.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Okay, thank you.

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

Dixie, one more question. This is David. I assume you considered granularity more fine-grained than section level and rejected that, is that the case? I mean, section is still pretty darned broad, all meds, all problems, those are sections. Obviously restrictions would be much more granular in the real world.

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

Yes, this is Johnathan. So, we did, and I wouldn't say that more granular restrictions were rejected outright. I think that we have, in our implementation guides, tried to describe a technical approach for being more granular than the section level, with the understanding that current implementations wouldn't readily be able to support that. Ioana, would you elaborate a little further please?

**Ioana Singureanu, MS – Eversolve LLC**

Sure. So where we – the CDA standard itself would not support a confidentiality code at the entry level, so for that purpose, the recommendation was to create an additional CDA template. But that CDA template, as Johnathan mentioned, does not exist yet. So while in the implementation guide we say that an implementation may include privacy metadata at the entry level, we know that for a fact right now, implementations do not, because that mechanism is not supported by the underlying standard.

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

So just, I mean, I know that the group is aware of this, but, obviously the way a lot of the structured documents get used, and in fact it's being encouraged by Meaningful Use Stage 2's requirement for the ability to incorporate or reconcile the inbound messages with structured data in the EHR itself, is that selected items are actually transferred into the problem list or the med profile from CDA inbound document. So, it's hard to imagine a workflow that works at the section level as restrict, as transferring the restriction of disclosure to things that get imported into detail structures of the EHR.

**Ioana Singureanu, MS – Eversolve LLC**

Yeah, the implementation guide allows for both section and entry level, so, you could be very granular if you so choose in supporting the templates that allow you to specify the security labels at the entry level. So that would be possible, of course.

**W**

... focusing ...

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

My concern is what would happen if a section is tagged – does that mean that you can't safely import any granular element into a place that does not, for example, respect these privacy codes and redisclosure codes?

**Ioana Singureanu, MS – Eversolve LLC**

Well if a section is marked as protected, theoretically you could consider all the entries may inherit the same level of protection.

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

Right...

**Ioana Singureanu, MS – Eversolve LLC**

Unless there are specific entry-level labels that are applied to each label, in which case, each entry would have its own privacy settings. So, that would be up to the implementations, and there's still work on the way to harmonize these requirements and make sure the underlying standards support them.

**M**

But ...

**W**

Ioana, this is ...

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

But wait a minute. I think we need to move on here. I think the questions have been answered, but I, respecting Johnathan's warning that we have a lot of slides to go through, let's move on.

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

Thank you. So this slide is another representation to show the nesting, essentially. So we have the building blocks, the confidentiality codes, any obligations such as prohibition on redisclosure and the purpose of use and then also please note that we do have transport metadata that is also applied here. And Ioana, if you want to make any comments on this slide before we ...

**Ioana Singureanu, MS – Eversolve LLC**

Sure, sure. I just wanted to emphasize that basically that summary document and payload could be replaced by any other type of payload, but the outer layer of mandate would still apply to those artifacts. So again, and this is just an example of how you would exchange information between two organizations, and the transport metadata would specify that this information is restricted, that it should not be redisclosed and it's intended for treatment purposes only, in this example. Multiple purposes could be enumerated, of course, but in this example, you have a specific example of metadata that is necessary to support the requirements of that exchange.

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

Thank you Ioana. So the next slide's going to look a little bit more clear to the system behavior. We did, during the course of the Initiative, for a while break out into three separate workgroups. One of those workgroups looked at system requirements and system behavior to the EHR systems that may be necessary and so in this diagram, on the left-hand side we have a representation of a sending system, and on the right-hand side, that's the receiving system. So there are certain characteristics of the sending system that we would expect would be that the sending system should be able to identify the information that it's going to be restricted.

So, back to our use case, that would be identifying information that is protected under 42 CFR Part 2 or Title 38, predominantly. The next step would be to verify that the patient's privacy consent allows for the disclosure of that protected information. And then adding privacy metadata to that health information, so that when it is disclosed to the recipient system, the receiving system receives not only the clinical data, but also the privacy metadata that has been applied to convey the restrictions. Conversely, the receiving system, the process of privacy metadata that's associated with that health information that they received. They would identify the third party protected information before redisclosing it and they, of course, would also have to verify the patient's consent in this case, before redisclosure of that protected health information also. So we do have sort of layered standards that we would use to try and make this happen.

On the next slide please, you'll see some of those mechanisms and capabilities, and we just listed it here in terms of the sending systems. So, identification of information that's further restricted. There are several ways to do that and our approach is to try and use all the means that are available within an EHR system to be able to make that determination. So for example, LOINC codes and ASC 5010 for healthcare provider and facility types and healthcare coverage type, SNOMED-CT for protected diagnoses and problems. So collectively these can be useful in helping determine which information is further restricted.

Secondly, verifying the patient's privacy consent allows for the disclosure of the information. In our implementation guide, we have two optional transactions, which are used in a health information exchange environment, where they would direct a query at a consent directive location and then actually request the consent directly, then retrieve the consent directly. And then also we would expect the system to be able to check the consent directive for the patient's consent, prior to making the disclosure. And we'll get Ioana talking more about the standards in a minute, but here we selected the HL-7 CDA R2 consent directive, which is still in TSTE right now, but we understand it's going through.

So, the third step in this diagram, was adding privacy metadata; we have our building blocks. So the HL-7 confidentiality codes for the CDA where we have the values here that are primarily used within our use case of normal, restricted or very restricted. We have the refrain code such as the prohibition on redisclosure and the purpose of use, which would support treatment, payment, operations or emergency treatment. We also have the ability to include a URL or XACML policy pointer for reference, if needed.

Okay, next slide please. All right, so at this point I'm going to turn it over to Ioana, who's going to talk a little bit more about those standards that were selected and have been incorporated in the three implementation guides. Go ahead, Ioana.

**Ioana Singureanu, MS – Eversolve LLC**

Thank you Johnathan. So, the next slide we're discussing the main building blocks of the privacy metadata proposed by this Initiative and just wanted to emphasize that throughout the Initiative we attempted, and I think we succeeded, in reusing a great deal of specifications and prior work to leverage for enhancing the interoperability specifications in existence. So we tried to leverage existing standards and where possible, to extend them so they are better suited for exchanging protected information. So the first specifications refer to confidentiality codes. And in this regard, we decided to reuse the HL-7 confidentiality code system and specify a limited value set that identifies information as very restricted, restricted or normal confidentiality. And that would be basically generic HIPAA rule data that would be exchanged for treatment, payment operations.

On the next slide, we are discussing purpose of use and the purpose of use concept and the associated terminology is used in several places. It's used in creating a user assertion when the information is requested from one provider to another. It's also used in the context of disclosing information when a push transaction is initiated and the purpose of use is asserted to the receiver of the data, the receiver has to use the data for the purpose intended. And it's also very useful in specifying a consent directive authorizing the disclosure of data for specific use to a certain provider. So, in all these uses we would like to see a consistent use of the terminology and the concept itself, so we have consistency. And again, I think this is a very helpful element for the implementers who do not have research the concept over and over again, but they have a single description and a single value set that is sufficiently representative.

So the third building block, the next slide...next slide please. Intents of obligations, it's something that is quite common in interoperability is that the receiver of the data has to often live by certain responsibilities as a receiver. It may involve sending an acknowledgement, it may involve persisting the data in a certain way. In this case, these are obligations regarding handling protected information, and they are encoded using very simple, very straightforward policy. So what we're doing really in this case is taking something rather complicated, like a 42 CFR Part 2 policy, and we're distilling this down to a very simple metadata for interoperability. So the idea is to simplify the distinctions and the differences across policies and resolve them down to privacy metadata. So a typical privacy ... refrain policy that would be applicable to a behavioral health provider exchanging information with another provider would be the addition of an obligation specifying that the receiver cannot redisclose the data without the consent of the patient. But again, there may be other obligations that could be included in there, so, the implementation guide refers unambiguously to value sets and coding systems that are applicable for encoding these types of obligation policies. And finally, on the next slide, we have an example of where this privacy metadata appears and emphasizing that this Initiative is not in any way different from other initiatives when it...in regard to the exchange of documents or messages. We're using the exact same mechanisms as other initiatives and other projects.

Next slide. Here's a summary of the standards and the profiles that have been reused and, as you can see, we are making use of the IXE XDS metadata to support the generic submission set metadata, but also the added privacy metadata. We are also making use of existing vocabularies in order to correctly segment the data and identify protected data segments. And this involves things such as the XL 5010 specifications to identify the type of insurance coverage for out of pocket payment, or the HITSP 80 value set for healthcare facilities to identify 42 CFR covered facilities. And the building blocks themselves are based on existing terminology and coding systems, primarily from HL-7 and harmonized with other standards development organizations.

Next slide. This is just a summary of the specifications that have been used without any change. And as I mentioned to you earlier, we are relying on the generic exchange of documents that is already in use, the direct and NwHIN connect mechanisms. And, where applicable, we're exchanging privacy consent directives also as CDA documents. So, it should be a relatively easy adoption and I think that some of the pilots have confirmed that it's relatively easy to incorporate this additional capability because it builds on existing transport and information exchange mechanisms. And I think that I'm going to turn the discussion over now to Johnathan, to discuss the accomplishments and the artifacts.

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

Yeah. Thanks Ioana. So if we can advance two slides please. So I'm going to talk briefly now about the accomplishments and the artifacts that came out of the Data Segmentation for Privacy Initiative and really shift our focus now on the work of the community and the work of the pilots. So next slide please. So, as an Initiative of the Standards & Interoperability Framework, we went through the S&I lifecycle and produced a number of documents and artifacts, some I think are typical of an S&I Initiative and others not necessarily so. The first of those is the use case document and if potential implementers are unsure about whether or not there is a need for data segmentation for privacy in, or capabilities within their environment, the use case document is a good place to go and look. Because it outlines a number of scenarios that we tried to distill down and describe the high level workflows for, and that we then used as the foundation to build our implementation guides.

Our first generation implementation guide tried to encapsulate different transport mechanisms and architectures, and it made the document fairly voluminous. So, the current iterations were to break the larger Implementation Guide down and distill it into those three areas; the first being SOAP oriented, which provides support for eHealth Exchange. The second really provides support for Direct implementations. And those two Implementation Guides are I think fairly mature. The third, which describes RESTful implementations, is still a work in progress and we'll be looking to get input from the standards community in particular on that one, as the standards become more mature and further, so currently we have three implementation guides and a use case document.

Approximately a year ago we also did an analysis of the Standards Committee parity and recommendations for privacy metadata and reported back on that analysis. So that's another artifact that the community generated. We have an executive summary document that outlines the conceptual approach and the use of the standards to implement data segmentation. That document is still in the community draft format, but it's going through some fine-tuning and I think is a much more digestible first read than some of the more technical implementation guides. And then finally, as shown on this slide, we have test procedures. So, two of our pilots went through a detailed requirement ... matrix that mapped their pilot implementations back to the technical conformance statements of the implementation guides, and these RTNs were used as a basis to help develop test procedures. So, the VA SAMHSA pilot right now is going through, and is continuing to go through, more rigorous testing against these test procedures and not only to be tests validate the pilots, but they also improve the quality of the test procedures themselves, so that they can remain as artifacts for our other pilots and future implementations to use, so that they can validate the data segmentation specific aspects of the solution. Note that the test procedures are not intended to replace the basic conformance testing processes and tools that are already in place to test the base standards. These test procedures are focused on the data segmentation capabilities.

Okay, next slide please. We did have 98 committed members and our community supports and we had 92 participating organizations throughout our 12 months of being an Initiative. In all we've had I think about 150 or so individuals participate on a recurring basis and obviously not 150 people show up on every call, but altogether we've had 297 participating individuals during the time that we've been tracking the participation throughout our community. And meeting for an hour and a half every week and sometimes when we've had our workgroups, we've been meeting up to three to four times a week as well. So, a tremendous amount of hours and effort has gone into the development of our work products.

As I mentioned, we're very proud to say that we've got five pilots, so one federal pilot and four industry pilots. The feds is the VA/SAMHSA pilot, and they were demonstrating the initial phase of their work under data segmentation at the HL-7 conference in Baltimore last year, and more recently, at the HIMSS 2013 Interoperability Showcase. Our next pilot also demonstrated as part of the ONC FHA interoperability showcase at HIMSS. The Software and Technology Vendors Association or SATVA, are also well on their way into going into production, more on that here in a moment. And then two of our newer pilots, the first is ... as the Jericho Systems University of Texas Pilot and the Greater New Orleans Health Information Exchange Beacon Community is now data segmentation and are implementing the initial stages of their data segmentation deployment. So, the next three slides go into a little bit more detail as to the current status and accomplishments of each of these pilots.

Next slide please. Okay, so beginning with the VA/SAMHSA Pilot and Mike Davis, who is on the call and on the Privacy & Security Workgroup, has been leading this pilot. So Mike, please feel free to elaborate on the slide as we go. Some bullet points here from SAMSHA's perspective, SAMSHA are extending and continuing the development of their open source Access Control Service. They're adding an informed consent user interface and by adding API's to manage the identity for the patients and the providers, they are looking to begin pilot testing this capability in October of this year. They're also translating the privacy protection policies into standardized clinical and social science terminology, and they're doing that through the HL-7 ballot of the summary behavioral health record and implementation guide, and the privacy consent implementation guide. SAMHSA's also able to implement privacy protections in the context of public health reporting or research by permitting or redacting more or less of the demographic or identity data, and this second form of segmentation is pertinent to the Structured Data Capture Initiative of the S&I as well. I'm just going to pause there and see if Mike has anything to add from the VA perspective on this pilot.

**Mike Davis – Veterans Health Administration**

Thanks Johnathan. So, yeah, I got my – I didn't get my comments in early enough to make the slides. So the VA has already implemented much...some of the infrastructure necessary to implement this. We've put in place an interface for veterans and patients to enter their consent directives electronically and digitally sign in using a VA supported digital signature service, with preapproved policies from here that automatically go to an access control system. The VA has also already implemented a federation system and access control system to manage these policies. The veterans currently are able to do basic opt-in, opt-out types of requests and we're soon putting into place an ability to do restrictions, organizational restrictions as part of the work. And our demonstration also went to demonstrate how entry-level classification markings and categories can be put on the information and address some of the questions that David was speaking to earlier. In my role as one of the chairs of the HL-7 Security Working Group, we've also initiated, in support of this, a healthcare classification system for privacy and security, which is currently in ballot, which will provide extensions to the capabilities that are being described here.

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

Thank you Mike.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Is that – it's a consent – informed consent on that last slide, in the VA slide? Yeah, I'm looking at the wrong thing. See where it says informed consent on the first bullet, is that the term informed consent is rarely applied, used when you're talking about privacy labeling, it's usually used with respect to informed consent for treatment or participate in research. What is it meant – what does it mean here?

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

So again Mike, look for you to elaborate here, but this is an example of a user interface that is in – I think in this case a browser based interface that allows the patient to make informed choices about what information they are allowed to further restrict the sharing of, and which they are not. And I think the idea here is that consumers or patients understand the implications of those choices and that the interface helps them understand the implications of their choices.

**Joy Pritts, JD – Office of the National Coordinator**

This is Joy, if I could just break in a minute. Dixie, this is what we have been referring to as meaningful choice.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Okay.

**Joy Pritts, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Health & Human Services**

Does that help?

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Yes, yes and yeah, that's – I'm pleased to hear that, too.

**Clement J. McDonald, MD – Director, National Library of Medicine**

Are we on discussion points, because – this is Clem – because I can envision another 40 hours a day to talk to the patient, explain things to the patient, patient lines growing longer and longer. I mean, this is an immense amount of decision-making that's brand new. Has anyone thought through the effort required to actually address these with the patient? Don't picture the web base working in an emergency room and don't picture it working with inner city patients necessarily very well. So, I mean I can see this being the sand that will stop all healthcare.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Who is this please, I don't think ...

**Clement J. McDonald, MD – Director, National Library of Medicine**

Clem McDonald.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Pardon.

**Clement J. McDonald, MD – Director, National Library of Medicine**

Clem McDonald.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Oh hi, hi, I didn't recognize your voice. Right now we're receiving questions only from the Privacy & Security Workgroup, so would you hold that question until the end please?

**Clement J. McDonald, MD – Director, National Library of Medicine**

Well actually I don't know what workgroup I'm on, I guess I'm not on that one – okay.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

No.

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

Thanks Clem, this is Johnathan. I've made a note of your question and we will definitely return to that towards the end of the call. Thank you so much.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Thank you Clem. I'm sorry, but we do have to enforce the rules here.

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

Okay, so next slide please. Okay, so it is impossible for us to try and articulate all the work that the pilots have done on a single slide for pilots, so again, forgive me, I'm just going to try and hit some of the highlights. And again, I'm the messenger here, the expertise and the real technical implementation level understanding of the choices that the pilots have made throughout their deployments, rest with them. So for right now, let's just talk about this at a fairly high level. So the SATVA pilot, which includes Cerner Anasazi, the Valley Hope Association, Defran Systems, and HEALTHeLINC.

So this SATVA pilot implemented the options in the Implementation Guide into specific implementations of the human readable narrative notice into the disclosures. And I think that that was a really nice add that this pilot brought back to the Implementation Guide, this human readable notice that is conveyed and pops up in their interface to require an acknowledgement from the human end receiver as the information that they're about to look at is subject to redisclosure restrictions. And then incorporation of the legally and contractually required obligation and refrain codes at the envelope header and entry level of disclosures, again in human and machine readable format. They're also implementing this not just in a point-to-point setting but using an HIE they're looking to communicate the CCD to the HEALTHeLINC RHIO in the Buffalo, New York region, and working very hard and tirelessly to get this into production. The Valley Hope Association member will also be beginning deploying the capturing of the consents online using...again using a browser application here, and then management of the Part 2 compliant disclosures, using the SATVA model. So several parts to this ecosystem, they've worked very hard and very rapidly, and are in the first and second phases of deploying to production. So, they should be congratulated on their efforts here as well.

Okay, next slide please. Okay the NETSMART Pilot. So this was the other pilot that demonstrated at the interoperability showcase at HIMSS 2013 and this ecosystem includes the Tampa Bay 2-1-1 Referral Network and the Kansas Health Information Exchange. And they're focusing on ensuring that all data is correctly tagged in the payload and the protocols used to transport. The receiving health information organization or EHR can properly enforce the policies associated with the sensitive nature of the data received. And they are implementing this with two different groups, so as I mentioned earlier, the first is the referral network in the – this is commonly referred to as the Tampa Bay 2-1-1 network, where they're implementing the first two scenarios from our use case, managing the direct push or pull information between the organizations. And then the second is with the Kansas HIE where they're working with behavioral health providers to implement the exchange scenario in our use case, where they're introducing the registry and repository model for the consent directives. And each of these groups will manage the restricted data associated with 42 CFR Part 2, which is their particular focus. Again NETSMART has, I think within about a 3-month timeframe gone from doing business the way that they have historically done business to being able to incorporate aspects of data segmentation for privacy into their production environment. So again, I think a huge accomplishment.

Next slide please. So the Jericho Systems/University of Texas Pilot is one of the newer pilots that joined our Initiative and they have a slightly different focus. What their primary focus is also in the exchange of clinical data with privacy metadata to show which data can be accessed or readily shared and which cannot. But they're also going to be looking at how the consumer can be informed of any requests and access control decisions that are made against the clinical data and then correlating that with the use of the consent directive.

Next slide please. And then our most recent pilot to join is the Greater New Orleans Health Information Exchange. So, already they are filtering sensitive data from entering in the CDR and exchanging that filtered information among their community member organizations. But moving forward, they're looking to integrate the previously filtered sensitive data and then be able to use the security labeling scheme of our confidentiality codes to help govern the use of that ... help govern decision-making for future disclosures of that data.

Next slide please. Okay, so we do have just a couple of conclusion slides, and then I think we certainly want to allow plenty of time for questions. So, next slide please. So the work of our community I believe has shown that data segmentation does provide a means of protecting specific elements of health information in an EHR and in the broader exchange environments, which we believe can prove useful in implementing current legal requirements and honoring patient choice. And again, please note that the focus here is...for our initiative, has been implementing current legal requirements. We did really try and stay out of the policy debate where we were often tempted to get involved, but the relative merits of various disclosure policies were outside the scope of our Initiative, and so we focused on those that were already current legal requirements. So while there is still work to be done and we know that our Implementation Guides cover an 80-85% perhaps solution, we're still looking to see the full outcomes of the pilots, but we are very hopeful that this data segmentation will improve...will facilitate improved sharing and integration of behavioral health information among the provider community.

So, next slide. We know that there are likely to be some extensions to some of the base standards and adoption refinement of the implementation guides with or by the standards community will really help, I think, accelerate the tweaking that needs to be done to the implementation guides and will accelerate the adoption of the IGs to allow interoperable solutions, so that the appropriate privacy protections can be put in place and can be implemented across organizational boundaries. And I think this is really key. There are lots of ways to do fine-grained access control using the EHR systems and using access control systems within an organization. But being able to apply these building blocks so that the information can be conveyed across organizational boundaries and using standards will have a strong sense of trust, that the receiving system will be able to interpret those vocabularies in the same way and to be able to apply the same level of rigor to protecting the patient privacy as was intended, when it was originally disclosed. So we hope that data segmentation will give patients the confidence that the privacy choices that they make, which they are allowed to make by law, by jurisdictional organizational policy will be honored. I think that concludes the main portion of our presentation.

And next slide please. So I just wanted again just take an opportunity to thank you for allowing me to present the work of the data segmentation for privacy community, along with Ioana our resident subject matter expert in standards and has been instrumental with members of the community in helping develop the test procedures and architect the technical solution. And I'd be remiss in not thanking Scott Weinstein who, even though he's not with us today, has been our ONC program lead and has really been a strong driving force in helping us get to where we are today. Scott is on rotation right now at the White House with the Office of the National Drug Control Policy, but we understand will be back towards the end of September. So, I want to thank Scott publically for all his work and leadership as well.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Well thank you, you Johnathan and Ioana and your entire team. This is obviously the result of a tremendous amount of work by a huge cast of people and we certainly appreciate you taking the time to brief us on it and your briefing has been very, very informative to us. Let's open – I know that some people on the Privacy & Security Workgroup were holding back their questions, knowing that Johnathan had a number of slides to go through, so, let's for a minute here stick with the Privacy & Security Workgroup and have you ask your questions.

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

So Dixie, this is Walter.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Yeah.

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

Can you hear me?

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Yes, yes.

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

Thank you. Well first of all, I want to say this really is a very impressive amount of work that the Initiative has done and having been engaged and involved in it from the standards perspective, I think it has demonstrated a number of interesting things that are important to be tested and shown. It has, in the first place, it has shown how internally organizations may consider handling the need to restrict access to and disclosure of certain specially protected data. It does get inside the organization to show how an EHR could and might be able to do that. The other one, of course, is the interaction with the patient's privacy choices and the consent management process and how that interacts with the data that is being requested to be accessed or disclosed. And then lastly, really the ability to, if the disclosure is permitted based on patient choices, able to attach to that data some information towards the receipt and to consume and security, and that information related to the consumer sources. But, it has demonstrated sort of the realm of expectations and movement across data in specific instances. It has also demonstrated how, I think, how complex this issue is really, when you look at the number of standards that are interacting and the number of profiles and elements that are interacting, and I really like the slide that shows the list of all the functionality and then the various standards being called upon. I think it really shows how much...how complex this process is. And it also shows, and I'm glad that Johnathan mentioned this at the end, it also points to the need to continue the work and continue to look for further applications and how that might work in other situations beyond the three ... primarily the three or two federal mandated situations that were tested.

I think what I wanted to just mention is that it's going to be important to, as we take this report and as a workgroup look into what are the outcomes of this, it's going to be important to evaluate, based on the maturity criteria and the analyses that have been done with respect to the standards, where things are with them and how much this is really something that can be scaled up to other applications. And then really link it back to the handling of health information that is done in provider settings that really go beyond specific type of categories of records, for example, behavioral health records. I know, and I think David and others have mentioned this, how difficult and how challenging it will be to look at any sort of granular level fragmentation or segmentation of the data when you look at notes and other elements of the medical record. And truly the risks of going down that path of looking at segmenting data at that level that would create a level of complexity for sharing the record outside of – for the provider that receives that record to be able to understand the full picture of a patient's condition. So, I really want to again applaud the effort and it has shown us how much, how difficult it is and it has also shown us some ways in which things need to continue to evolve in terms of standards and the application of these to health information exchanges.

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

Thank you Walter, you touched on a couple of really, I think, really important and hot topics there. But I think that the building block approach that we've tried to distill this down into will help support a much wider range of privacy policies than those that we focused on during the development of the Implementation Guides. So those policies that we chose, the 42 CFR Part 2 and Title 38 primarily, were well understood and already required for certain organizations. So, it made sense for us to focus on those within our use case. But again, the assembly of the different refrain codes and obligation codes and confidentiality codes, using those building blocks, hopefully organizations will find are not that complex, so that as other jurisdictional privacy policies come into the mix within implementations, they will be able to be accommodated using different combinations of those same building blocks and vocabularies.

And I think that even though it can be overwhelming and sounding very complex, the fact that we have two of our private sector pilots so rapidly adjust their current way of exchanging to accommodate this privacy metadata to show that it can be deployed into production. And we're still waiting on the full evaluation, of course, so the jury's not completely out yet, but it does hold a lot of promise. And certainly the work of the standards community to add a more elegant, more refined and more eloquent way of stitching these building blocks together, we very much look forward to and welcome and need that input from the standards organizations, to be able to do what may be best. And finally, I think that the subject matter expertise in actually implementing and knowing truly what works well or what doesn't, within data segmentation, that skill set, that expertise lies within those who have been involved in the pilots. And so as we move forward and we gather more evaluation and feedback from the pilots, we very much look forward to turning to our pilot participants as being the subject matter experts to help guide us and help guide the standards experts into articulating the solution in a way that is more readily implementable by future adopters. So thank you Walter, you really, I think you narrowed it.

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

Thank you. Thanks Johnathan.

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

Dixie, this is David.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Yeah, hi David.

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

I'll just jump in here and make a few more comments. First, in terms of stuff that I really like and appreciate the hard work of an awful lot of people, in particular around the clarification of some of the coding schemes that can be used to describe the degree of confidentiality, the purpose of use and the restrictions that may or may not exist on the data. I think that work will be very valuable regardless of the rest of the framework and how it plays out. And in that context, I would just say that we have to be cognizant, in terms of Meaningful Use Stage 3 and EHR vendor certification and the like, to make sure that we don't let the perfect be the enemy of good enough, and implement requirements that are so complicated in their totality that we can't benefit from some of the advances in focused areas, like the clarification around these confidentiality codes.

The second concern I have is what I would call the analog hole and the impact on actual workflow of actual clinicians, and I'm hoping that we will in fact learn from these pilots. But, you could look at this a screen door with a big hole in it in that still today the vast majority of clinical knowledge is communicated in textual documents. And if we go to great lengths to manage the transmission and retransmission of structured elements, but don't address or can't address, the textual representation of that same knowledge, I don't know that we've done our patients as much good as the effort will be required to do all of that management of those coded terms. So, the analog hole is a real problem and I don't have a proposed solution, but I just say we have to keep that in mind, that solving the structured problem without solving the analog problem may not get us as much benefit as we think.

Then third, just to emphasize Clem's point about impact on workflow. I can imagine a scenario where, for example, a physician receives a CDA where the medication section is flagged as restricted redisclosure. But it's a complete list of every medicine that the patient is on, including, perhaps, some sensitive medicines, and he now wants to incorporate that into his EHR and the EHR follows the rules and flags everything that got incorporated as restricted disclosure, including his aspirin once a day and his beta blocker. How in the world are physicians going to deal with that workflow when the tags are associated at such a high level and the restrictions are, in fact, something completely different? I think we have to take that into account before we push this into the mainstream.

And then finally, I appreciate the decoupling of the codes from the transport. I think that future transport approaches will be very different from the ones that we currently use. I think we'll be moving more in the direction of things like FHIR and others that abandon the RIM and the EBXML constructs, because most of us agree that they haven't added very much value to the actual transport mechanisms. So, it makes good sense to keep a strict separation between flagging the data versus encumbering a dependence on understanding how the transport works. And I'll stop there.

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

Well thank you David, I really appreciate your comments. And so, I guess a couple of points. The workflow issue that you raised and I think that Clem also raised, is a really important one. We do have within the NETSMART Pilot and the SATVA Pilot, but particularly right now with the NETSMART Pilot, behavioral health providers actually involved in the pilot and in the exchange of information. So I think that a lot of the true workflow concerns that may exist, we have the ability to identify what those are and to capture them and to potentially work through. So, I'm acknowledging that they may exist, but right now they haven't been fully, I guess, articulated back to us, because of the stage that the pilots are in. As far as the emergency room access goes, and I think that was something that Clem mentioned, our use case does take into account emergency access to clinical data and the break-glass situation, which allows access to the restricted information, has been articulated and included within the Implementation Guide, and are also being demonstrated by the pilots. So, I think that that's encouraging and that that concern has been accommodated technically and from a workflow standpoint.

As far as your I think really good point about tagging medications and having the whole medication list be prohibited from redisclosure, we discussed that at length within the community and we think that there are multiple approaches that can be put into place to prevent that situation where every medication is suddenly prevented from redisclosure. So, that work, that discussion is documented. It is, in think, addressed in part in the Implementation Guides, but briefly, we have the ability to use very detailed, entry level tagging where systems allow for that, and I think the VA/SAMHSA demonstration is one example of that. But secondly, there are, I think, automated workflows that can be put into place so that you could, for example, I'm not necessarily advocating one particular solution over another here, just sort of summarizing some of the discussion that was had within the community. So for example, you could have one document that is sent that contains only the restricted information and is marked as restricted, and then another document that contains the information that's not subject to further restrictions, and that could be more readily incorporated into the receiving system. So, I understand that that may not be ideal either, but it is a potential solution that has been discussed and endorsed by some within the community.

**Ioana Singureanu, MS – Eversolve LLC**

If I may clarify something, Johnathan, this is Ioana. The fact that something cannot be redisclosed doesn't mean that the intended recipient cannot use it, I think that may be a misperception. It simply says that if the recipient of this data from a third party chooses to redisclose it yet to someone else, they would have to ask for a consent. So, it actually makes it easier from a workflow standpoint, because the EHR is aware that this is information that was not originated by this, here at this facility, but at another facility, and it has these additional restrictions associated with it. So the EHR does not have to alert the clinician unless the clinician is attempting an operation that's not authorized. So, in many regards ...

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

Yes.

**Ioana Singureanu, MS – Standards SME, Data Segmentation for Privacy Principal, Eversolve LLC**

... actually I think this privacy metadata will make the handling of this information much easier, because it will not be the responsibility of the clinician. EHR will have sufficient metadata to make correct decisions and that's what we tried to accomplish, to distill down these policies to a set of instructions to the EHR such that the EHR can assist in this workflow.

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

But my point, Ioana, is that if the tagging is coarse-grained at section level for example, you could pollute the entire contents of that section because the system will have no way of knowing which of the elements were really the sensitive ones and which of the ones weren't. And then any downstream support for feeding data to an HIE or responding to a targeted query, as per the Meaningful Use Stage 3 intentions, would essentially require now the whole medication list to be flagged as sensitive, even though in fact that was not the intent of the system.

**Ioana Singureanu, MS – Standards SME, Data Segmentation for Privacy Principal, Eversolve LLC**

Right.

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

And the notion that providers would create two separate documents is problematic, just, I mean, boy, I'd have a hard time selling that to ...

**Ioana Singureanu, MS – Standards SME, Data Segmentation for Privacy Principal, Eversolve LLC**

Just to be clear, the granularity of the data is clearly subjective, the granularity of the data in the payload. So, if you're exchanging text information that does not have any additional metadata in any way of distinguishing protected and unprotected data, then you have to mark that whole text artifact as being protected or not protected. You have no way of discriminating or segmenting out specific chunks...

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

Yeah, I agree that's a problem. That's the analog hole and if, in some settings of care that's not a problem because the text is restricted to ...

**Ioana Singureanu, MS – Standards SME, Data Segmentation for Privacy Principal, Eversolve LLC**

Exactly. So ...

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

... non-disclosed information. But in other settings of integrated care, that's going to be a bigger problem.

**Ioana Singureanu, MS – Standards SME, Data Segmentation for Privacy Principal, Eversolve LLC**

So in some cases you have granularity that is entirely at the document level, and as Johnathan indicated, in other cases you can have granularity at the section level ... be sufficient. And if that's not sufficient, then you have to use granularity at the individual data element level. So, it would have ...

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

That's not in your current proposal, you said, that the discrete level and I'm just pointing out that's a fatal flaw of the current model.

**Ioana Singureanu, MS – Standards SME, Data Segmentation for Privacy Principal, Eversolve LLC**

Pardon?

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

I think the absence of the ability to specify at the discrete level may be a flaw of the current model.

**Ioana Singureanu, MS – Standards SME, Data Segmentation for Privacy Principal, Eversolve LLC**

No, again ...

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Ioana, I really need to interrupt this because I want to give the other two workgroups an opportunity, this is an hour and half call, and I encourage you and David to talk – that for us, it's obviously a very important topic, very, very important. But I do want to give the other two workgroups an opportunity to comment here. Clem, why don't we start with you.

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

Dixie, this is Leslie. I do have a comment.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Yes.

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

So one of the things that I'm encouraged by is the ability to start looking at the future role of the patient in decision-making transitions of care that potentially be construct of informed consent or informed decision-making can make. And I think that this as a beginning step of an infrastructure to accommodate that patient flow is an important one. And I hope that although it's quite foreign and difficult to think of it in today's provider workflow, I think as we evolve and the patient is much more active and integrated into these transitions of care or movement of data, that this allows for a robust sharing of very specific and decision and actionable data for the patient, beyond just the restricted use of data as defined here. So, I would commend the group on forward thinking and the future use of this infrastructure could be important with regards to patient engagement. Thank you.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Thank you Leslie. Clem, let's go to you.

**Clement J. McDonald, MD – Director, National Library of Medicine**

Well, I think the proposal is elegantly ... an elegant technical proposal. So from a technical perspective it's beautiful. I still think it'll be a disaster in operation for patient care unless we carefully put boundaries on it and that currently we can handle the issues. If it's a drug treatment program, it just doesn't come over and that's not so hard to deal with. But this whole bit – and psychiatric it's just the psychiatric notes, it's not the drugs and all the rest. So we shouldn't get it all mixed up. I would actually, as a clinician, if a patient won't let me see all the drugs, I couldn't see them, I mean I'd kill them by accident, I couldn't take that risk. This will also create a very large legal burden on institutions if they screw up, once they've committed to such protection. So maybe I'd like to hear some discussion of some practical pragmatics. How would this be applied in real life? Now I can see how a drug treatment ... could just label everything they have and send it out, one of the alcohol or drug abuse treatment programs. But tell me how this is going to work in clinical care? A patient's going to check off each box, they do or don't want to send to anyone else before they leave the room?

**Jamie Ferguson – Kaiser Permanente – Vice President, Health Information Strategy and Policy**

So Dixie, this is Jamie. I just wanted to put my card up as well.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Okay. Hi Jaime.

**Joy Pritts, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Health & Human Services**

Dixie can I – this is Joy. I'd like to respond to Clem, because it is a policy issue that he's raising.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Um hmm.

**Joy Pritts, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Health & Human Services**

And we purposely kind of steered away from – we recognize that the technology here could be used for a broader scope of use cases than what were presented. But where we are today really is that there are a series of laws both at the federal and state level that give patients, that prohibit the disclosure of certain patient information without the individual's consent. And what is happening right now is that these patients are being excluded from health inf – the development of health information exchange and health information technology. So the primary purpose of this project was to look at current laws and see how we could implement them electronically. That's pretty much what this...

**Clement J. McDonald, MD – Director, National Library of Medicine**

Well that makes me a little relaxed, but I think if one – if you present this, it might be good to give a scenario for one of those specific cases. And actually, it doesn't prohibit the patient, it prohibits the data at the treatment center or the data, and the discussion of HIV and all getting thrown into it is really confusing. Because again, as a physician, that's a crucial data element for care and if that's hidden, we're going to ...

**Joy Pritts, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Health & Human Services**

Well, we won't go into – what we looked at is when we looked at what laws were out there that said to a provider, you can't share this information with others without the individuals specific consent, HIV was among them. We focused the use cases in this project on the federal use cases, because obviously they are the most broadly applicable. I think that it's safe to say that nobody thinks that our work in this area is anywhere near done, and that there aren't policy issues that remain. But one of the things that we believe is that the technology should follow the policy and we shouldn't be setting policies such as we're not going to integrate behavioral care information into primary care, because we don't have the technology to help facilitate that.

**Clement J. McDonald, MD – Director, National Library of Medicine**

Well, as a primary care doc, if you could make it – to process, I'd rather give the behavioral health information and just gather it myself. What you're going to have is ...

**Joy Pritts, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Health & Human Services**

Well that's why we're doing the pilots, because in the pilots in particular, they will be having behavioral care providers actually sharing the information with GPs.

**Clement J. McDonald, MD – Director, National Library of Medicine**

I mean the problem with more granularity actually is a challenge of marking it and who's going to decide in all the gray zones? So, I just didn't want...someone should pay attention to not the workflow which we always thing about re-routing, but the time cost of dealing with separate elements, making decisions by multiple parties. I think primary care is in crisis now, people can't get Medicare...you can't find people who take Medicare, this is going to kill primary care if it slows them down.

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

This is Peter Kaufman can I make a comment?

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

I think Jaime is in the queue ahead of you Peter.

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

Okay, great.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Let Jaime go first and then – now, our call is over right now, I mean, technically, but I'm – let me see, I'm – MacKenzie, I know we have to open this to public comment, do we have to open it before 9:30?

**MacKenzie Robertson – Office of the National Coordinator**

So, we can take another five minutes, we don't have another call scheduled after this, so we can go over a little bit, but we do just want to make sure we're keeping somewhat to the agenda. So, I think maybe ...

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

We'll have public comment when we finish, but I'd like to give people an opportunity to ask their questions.

**Jamie Ferguson – Kaiser Permanente – Vice President, Health Information Strategy and Policy**

Yeah, I'll be quick. This is Jaime Ferguson. I just wanted to raise the issue that sometimes the nature of the blanket sort of consent flag could be problematic. And I think that the federal behavioral health restrictions are actually the exception, whereas the rule, or the more frequent application of the technology would be more likely in state or other jurisdictional requirements having to do with the redisclosure. But if that then flows over to a provider who's operating in a different state or a different jurisdiction that doesn't have those same redisclosure requirements, then the blanket consent really is problematic for those kinds of use cases.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Okay. Peter?

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

Mine is almost the opposite comment. I've been in practice for over 25 years and I think the vast majority of patients want the best care they can have, which includes sharing of data. There are certainly some patients who are very concerned, and we should try to avoid laws that limit the possibility for easy sharing of data without a lot of extra work, for the vast majority of patients that are not as concerned about sharing their healthcare data. So for example, I think there should be a blanket approval included, we should not have a law that says no, no, it has, like in some states, that you have to have a separate approval form for this data, for behavioral data, for HIV data, for narcotics data, things of that nature. We should allow, at least nationwide, a blanket approval for those patients, who I believe are in the majority, that would like their data to be shared easily and without the doctor having to run through a lot of hoops that'll keep him from doing it.

**M**

Here, here.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Yeah, I heard that comment many, many times and especially from patients who are really eager to allow their information to be used for research and they find it difficult to do that. So, I'm glad you asserted that Peter.

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

This is Johnathan, just real quick, just to sort of piggyback off of the last couple of comments. I really appreciate all your comments, but the – again, you heard me say before and Joy mentioned it, we did not debate the merits of any particular policies that exist, we were trying to architect a technical solution that would allow electronic implementation of these various disclosure policies. So, if the policy says, share it or don't share it, then hopefully our solutions will accommodate those. But ultimately, it's our belief and hope that the solutions that we're proposing here will actually allow data to flow more freely, rather than saying the EHR systems and health information exchanges can't handle this private data, so don't send it at all. We want the information to be able to flow more freely with the appropriate protections in place, so that the consumers and the patients know that it is being handled according to their existing rights. So, thank you.

**Paul Egerman – Businessman/Software Entrepreneur**

This is Paul Egerman can I ask a question?

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Hey Paul. Yes.

**Paul Egerman – Businessman/Software Entrepreneur**

The question I have is – I think first a comment is, I agree with David's observations. There's potentially a lot of workflow issues here that are very serious issues, and I can think of a couple of issues that David did not raise. But my question is, is among these pilots, when will something be in actual production and operation where patients are being treated and they're asserting their preferences and those preferences are being honored and things are not being redistributed. I couldn't quite see that in the pilots, as to when we would be able to see that, because I think that's the point where you have the real learning.

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

Thank you. So two of the pilots are going through a phase deployment to production right now where they are – they're starting, I think, primarily with direct and then integrating the NWHIN protocols and the pull scenarios. So, to the extent that two of our pilots are going into limited production as we speak, and they're adding additional capabilities as we speak and throughout March and April, is the feedback that we've received from the pilots.

**Paul Egerman – Businessman/Software Entrepreneur**

So through March and April. So in the month of April, patients will be seen and preferences will be recorded and EHR systems will be making decisions based on that, is that what I'm hearing?

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

That's my understanding from the work of the pilots to date, but again, please understand that this – these are – the pilots are in control of their own destiny here, and I have no insight or oversight on that particular project. The other thing that's worth noting is that within the Data Segmentation for Privacy scope, we have a pre-requisite that a fully reconciled, adjudicated and a legally acceptable consent directive is what is provided to their decision making service and that the workflow associated with obtaining that consent or revocating or updating the consent is again a workflow that was out of scope of our particular Initiative. Thank you.

**Paul Egerman – Businessman/Software Entrepreneur**

Thank you.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Will patients be told that that's – in that pilot, will they be warned that they're preferences may not be enforceable in other organizations?

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

I think that's ...

**Mike Davis – Veterans Administration**

This is Mike Davis ...

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

Go ahead Mike.

**Mike Davis – Veterans Administration**

I'd like to address a little bit of these questions because the VA is currently implementing some of these. We have a number of pilots in operation at this time, and we've put in place a lot of the infrastructure necessary to support all of, to support this. With the caveat that we're stepping into it gingerly and we're providing patients with the ability to express a limited number of authorizations and restrictions, and providing an infrastructure of support for them, to make sure that they're aware and understand the – what the consequences of their authorizations and restrictions are. We have to recognize that under the current laws, it's possible that the patient would decide not to share anything, because of their concerns rather than risk the exposure of certain protected information. So, this system provides them with the ability to have some recourse, so that they can share some information and not share others as allowed by law.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Are there other questions?

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

Yes, just a quick note, Walter here. But Mike, I think the current laws except for again 42 CFR, there's no current law, federal law anyway, that mandates that if a patient wants to restrict all of their health information from being disclosed, the provider must abide by it. The provider, the patient can request that, the provider has the ability to decide whether they agree with it or not. There are some state laws, again, that require that a patient consent be issued before disclosure happens, and in some cases, even before...or for treatment, payment and operations. But, as far as I know, there are no blanket applications of a case where a patient can restrict altogether the disclosure of data, again, except for this federal laws that protect special sensitive information.

**Mike Davis – Veterans Administration**

Walter, my comment was against the – are there currently operational systems in effect that are capable of enforcing what the data segmentation was and I was describing VA's efforts there? Johnathan already made the comment that the intent of our approach was not to specify what policies would be enforced, but to provide an ecosystem where, that was capable of supporting a variety and a number of policies. And so, my comment was not to the policy issue, but to the question of whether there were actual implementations in effect today.

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

Some of those flags that a record might carry from a disclosure might be in other settings, the recipient of that data might take it as informational only, if you will, because that recipient might not be, as it's been mentioned a few times, might not have to abide by that flag, they might have a different organizational policy or a different jurisdictional law that that's not required, for example consent. So if a flag comes in for some data saying this patient, this data requires consent. Well, that data in that other setting, in that other jurisdiction might not require it and so, that flag might be informational only.

**Mike Davis – Veterans Administration**

Again, this is a policy matter. So, as a condition of the disclosure, the disclosing organization may require as an obligation on the receiver that they honor the policies, otherwise we won't give them the information. That can be done by MOU or by some kind of exchange, okay, so ...

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

Yeah.

**Mike Davis – Veterans Administration**

... there is a way of doing that. And the patients themselves, particularly for certain kinds of information, may be allowed to decide whether or not they want to share their information. So the VA has, for example, adopted an opt-in/opt-out approach to eHealth Exchange, giving patients the right to determine which organizations they do and do not wish to share information with, regardless of the type of information.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Okay. I think – we’ve gone 10 minutes over, unless there is someone out there who has a burning question that they must get asked right now, I think that we should open it up to public comment. But first I do want to thank Johnathan and Ioana and your entire team for this work and Joy, thank you all for the work that you’ve done and thank you also for your time today in preparation as well as presenting this work to our workgroup. So, with that, I think MacKenzie we are ready for public comment.

**Public Comment**

**MacKenzie Robertson – Office of the National Coordinator**

Great. Operator, can you please open the lines for any public comments?

**Rebecca Armendariz – Project Coordinator, Altarum Institute**

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

**Operator**

We have a public comment from Michael Peterson. Please proceed with your comment.

**Michael Peterson, MD, PhD – University of Wisconsin**

Ah yes, this is Michael Peterson. I’m a hospital psychiatrist in Madison, Wisconsin, at the University of Wisconsin. Similar to what Dr. McDonald mentioned, concerned about the practical matter of implementing further restrictions and also concerned that having more restrictions for behavioral health records in particular is going to compromise patient care and create a more dangerous situation. We see some of that here where we’re trying to work on a break-glass functionality to meet some of our state guidelines, and also concern that it’s rather going to perpetuate stigma and separateness of mental health care rather than improving or decreasing that.

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

Thank you, Michael. This is Johnathan. Just to sort of to reiterate, and I’ll I ask Joy to please help me out here if she feels I need to be helped out. Again, we are not trying to get create new policy, what we’re trying to do is to electronically implement policies that already exist and our focus has been those policies that are required by law. So again, we’re not introducing any new requirements to share or withhold information that don’t already exist today.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Any further public comments please.

**Operator**

We have another public comment from ...

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Johnathan, you are not required to respond to every public comment.

**Johnathan Coleman, CISSP, CISM – Security Risk Solutions, Inc.**

Oh, thank you.

**Operator**

We have a public comment from Zorba Paster with Dean Clinic. Please proceed with your comment.

**Zorba Paster, MD – Dean Clinic**

Ah yes. My name is Zorba Paster. I'm a family doc in Oregon, Wisconsin and I want to give an example that happened yesterday on why data should not be segmented. I had a patient who came into my office, new patient I hadn't seen before. He was somewhat dizzy and had bleeding per rectum. And so because in Wisconsin, where we are, everyone's on Epic, pushed a couple of buttons, within a minute I was in his University of Wisconsin record. At that point I could see indeed, that his blood pressure was low, 98/60, his blood pressure was high at the last visit there. I could look at his hemoglobin and see there was a major change in his hemoglobin. I asked him if he had had a colonoscopy and he said, I couldn't remember, they put a tube there, but I was partially awake, he had not had a colonoscopy. I could see that he was on Indocin, which he forgot to tell my nurse, which was a possible cause of his GI bleed, but wasn't ultimately. And so before I sent him to the colonoscopist, our GI doc to see him, I looked through the rest of the chart and saw indeed, he had another factor that he hadn't explained, which was atrial fibrillation. So if there were data segmentation, I might not get all that data. I did it in one button and that's what counted.

Number two, I happen to be head of our IRB and have been head of our institution review board for 25 years. We had a morning meeting today discussing just this. If somebody is on one of our studies at our clinic, and if they end up at the University Hospital, and if they have something, for example, serotonin syndrome, because we were talking about a drug that can produce serotonin syndrome, with a touch of a button, they can look into our record and see what that patient is on. So, I think it behooves us to really have data that can be looked at very quickly.

The last comment, because I've listened to this for about a half an hour, I don't have the time to segment data into one spot versus another spot versus another spot. As it is, as a family doc, I want to spend more and more time with my patients and if you think that I'm actually going to segment it into different spots, I'm not going to do it. So ultimately that segmentation is going to either go to somebody else at the Clinic who won't do a good job, or it won't happen. And when you don't have the exchange of information, you're losing something that I think is critically important to 2013 and 2015 medical care. Thank you.

**MacKenzie Robertson – Office of the National Coordinator**

Thank you. And I believe we have one more final public comment.

**Operator**

From Larry Garber with the Reliant Medical. Please proceed with your comment.

**Lawrence Garber, MD – Reliant Medical Group**

I thank you. This is Larry Garber, I'm an Internist/Medical Director for Informatics at Reliant Medical Group and wearing both of those hats, I'm concerned with my ability both to truly segregate the data. And the other is, to be able to predict what the harm will be if I were to send data that is not the complete set of data on my patient. So a partial med list or part of the test results. So if I myself don't understand the implication of sending partial sort of Swiss cheese medical records, then how can I explain and get informed consent from my patient about the implications of sending that, and having them sign a truly informed consent. So while they could make a meaningful choice, I don't believe that they can truly make an informed consent.

**MacKenzie Robertson – Office of the National Coordinator**

Thank you very much and I don't believe we have any more public comments at this time.

**Dixie Baker, MS, PhD – Martin, Blanck and Associates – Senior Partner**

Okay. Thanks to everyone who dialed in today and thanks for our speakers.

**MacKenzie Robertson – Office of the National Coordinator**

Thank you everybody.