

**Privacy and Security Workgroup**  
**Draft Transcript**  
**June 29, 2012**

**Presentation**

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

Thank you. Good morning everybody. This is MacKenzie Robertson in the Office of the National Coordinator. This is a meeting of the HIT Standards Committee's Privacy & Security Workgroup. This is a public call and there will time for public comment at the end. The call is also being transcribed so please be sure to identify yourself before speaking. I'll now take roll. Dixie Baker?

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

I'm here.

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

Thanks Dixie. Walter Suarez?

**Walter Suarez, MD, MPH – Kaiser Permanente**

I'm here.

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

Thanks Walter. John Blair? Anne Castro? Tonya Dorsey?

**Tonya Dorsey – Blue Cross and Blue Shield of South Carolina**

Here.

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

Tonya Dorsey, are you on the line?

**Tonya Dorsey – Blue Cross and Blue Shield of South Carolina**

I'm here.

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

Okay, thanks. Mike Davis? Lisa Gallagher?

**Lisa Gallagher – Healthcare Information & Management Systems Society**

Here.

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

Thanks Lisa. Chad Hirsch? Jeff Jonas? Ed Larsen? David McCallie?

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

Here.

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

Thanks David. John Moehrke?

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

Here.

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

Thanks John. Sharon Terry? And is there any staff on the line?

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

Will Phelps.

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

Good morning, Will.

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

Hey, MacKenzie.

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

Joy Pritts.

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

Thanks Joy.

**Scott Weinstein, J.D. – Office of the Chief Privacy Officer, Office of the National Coordinator/  
Health and Human Services**

Scott Weinstein.

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

Who was that last one?

**Scott Weinstein, J.D. - Office of the Chief Privacy Officer, Office of the National Coordinator/  
Health and Human Services**

Scott Weinstein.

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

Oh, thanks. Okay...

**Stanley M. Huff – Intermountain Healthcare**

This is Stan Huff; I'm here as a guest today, too.

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

Okay, thanks Stan. Alright Dixie, I'll turn it back over to you.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

Great. Thank you all for dialing in today and for our guests. Stan, I'm glad you could join us. Are you here for Chad Hirsch? No, you wouldn't be, never mind. But I'm glad you could join us. At any rate, this is a meeting that Joy Pritts has requested to tell us about the work that her office has been doing around data segmentation, so, I know that all of us on the line are eager to hear about this work Joy, so, thank you very much for setting it up, we appreciate it.

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

Well, I'm going to turn the meeting over to the people who have actually been doing the work, which is Johnathan Coleman and Scott Weinstein, who has been supporting him. The work that we have been doing has been done through...in conjunction with the Office of Standards and Interoperability, S&I framework. So, it has been a joint effort and I will turn it over to Johnathan.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Yes, thank you Joy and good morning Dixie, Walter and members of the workgroup. We're very grateful for the opportunity to present our work here today. And please know that there have been hundreds of hours of collaborative work that has gone into our work so far by the community at large; and I think some of our community members are also participants on this workgroup and have put in a considerable amount of time and effort to get us to where we are today. So, in particular, I think we should mention that John Moehrke, Kathleen Connor, Joana Singureana, Walter Suarez, Mike Davis and Richard Thoreson are among those people who have really contributed to the material that we've got so far.

So, I have the enjoyable task today, with Scott, of presenting the collective thoughts of the group so far, to this group. Also, please know that as we go through the material today, that our proposed approach here is not fully complete yet. The Data Segmentation for Privacy Initiative is still a work in progress. We're teasing out some areas and are currently going through consensus voting on our implementation guide and resolving the comments from the votes that we've received. But, as I said, we're very pleased to be able to present to you today. I am Johnathan Coleman, the Initiative Coordinator. Scott Weinstein, from ONC, has been really guiding us through this project as well, and Erik Pupo, who's also on the line, is a subject matter expert and the Harmonization Team Lead for our Initiative on the Standards and Interoperability Framework. So, as we go through the material today, please do feel free to stop me at any time, ask questions and Scott and Erik and Joy, of course, I invite you to speak up wherever you feel appropriate also.

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

You know I do, Johnathan.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Okay, so Dixie and Walter, if you don't have any other remarks for us, if you like I can get straight into the presentation material.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

That'd be fine, thank you.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Thank you.

**Walter Suarez, MD, MPH – Kaiser Permanente**

Yes, go ahead, go ahead Jon. Thanks.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Yeah, thank you Walter and good morning. So the presentation today is sort of two-fold. We'd like to present the data segmentation for privacy approach as it stands today, and I'll get into a little bit more about our approach and what data segmentation for privacy is all about. But also the community has been able to compile a response to the Standards Committee's analysis and recommendations on patient privacy provenance and identity metadata. And I'm also very glad that Stan is on the call today, because some of our comments in this presentation will be in a reflection on the recommendations from the Standards Committee and the Power Team's recommendations from June last year. So, next slide please.

So, our proposed approach. First of all, just very briefly, what is data segmentation for privacy? It is an initiative that we're working on and it aims to address the standards needed to protect those parts of the medical record that are deemed especially sensitive or that may otherwise require additional privacy protection, but still allow other health information to flow more freely. So, that's kind of the general sense of what data segmentation is for. Sounds simple in the outset, but as we've learned through our workgroups meetings so far, it's actually much more challenging than one might first think. So, next slide please.

This slide and the next slide are very distilled, generic use cases of how data segmentation might come into play. So, of course we do have a very comprehensive use case document that outlines the specific scenarios that our initiative is addressing, but these two slides are a general, high-level view to explain very high-level of the type of workflow that might create data segmentation. So in this example, a patient receives care at their local hospital for a variety of conditions, including substance abuse, as part of a covered 42 CFR part 2, alcohol and drug abuse treatment program. Now that's important; the fact that this is a 42 CFR part 2 covered program is what triggers the enhanced protections to come into play. So not every encounter that involves alcohol or drug abuse is automatically subject to the requirements of the law for protecting that data in an enhanced way. And Scott and Joy, of course, are our legal experts on the line here, but the fact that it is a covered facility is what triggers the 42 CFR part 2 rules to kick in effect, in this particular example. Scott, is there anything else you'd like to add on 42 CFR part 2, specifically here, before we carry on?

**Scott Weinstein, J.D. – Office of the Chief Privacy Officer, Office of the National Coordinator /Health and Human Services**

Just that we've also...while we've been able to provide some advice on 42 CFR part 2, we've also relied on SAMHSA's guidance, and they've been very involved in this project, in terms of working on our 42 CFR part 2 use case.

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

SAMHSA is the regulatory agency that has promulgated that rule.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

I have a question, Johnathan.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Yes.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

This is Dixie. You said a 42 CFR part 2 facility, are these always dedicated facilities or are there doctors whose practices are authorized to do encounters under this program?

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

That's a great question. Scott, why don't you answer that one, if you don't mind.

**Scott Weinstein, J.D. – Office of the Chief Privacy Officer, Office of the National Coordinator /Health and Human Services**

Sure. Yes Dixie, it can also be individual doctors whose practice hold...they hold themselves out as providing substance abuse treatment, and they receive Federal funding, which can be in the form of Medicare funding even. But those are the two main requirements; that they receive some kind of Federal funding support and that they hold themselves out as providing substance abuse treatment.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

Okay, that's helpful. Thank you.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Thank you. So, in step two here...

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

Johnathan, before you go on, I'd like to make one example, a contrary example because this one keeps coming up repeatedly. So, just for clarification. So for example, if an individual goes to their regular primary care provider and that primary care provider, they just happen to tell them, "I think I have a substance abuse problem," or "I'm drinking too much," that doesn't trigger this requirement, because a primary care provider isn't holding themselves out to be a substance and alcohol abuse treatment provider.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

Thank you.

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

This is John Moehrke. I would just like to interject one other attribute. Although these were the minimal use cases we were asked to support in the data segmentation for privacy, we did look more broadly to make sure that the technology that we chose could support other sensitive topics such as genetics under GINA or HIV or other particular sensitive topics. So, not to say that we only focused on this one, because one would, indeed, be pretty easy to deal with, it's very facility oriented and not so much topic oriented. But, we did look to the more broader concepts of sensitive topics.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Yeah, thank you John. That's absolutely right. We chose 42 CFR part 2 in part because it is a broadly recognized, universally recognized requirement that we wanted to use as a baseline policy or requirement. But we did want to make sure that our proposed approach that we'll get into here in a moment, is extensible and can accommodate other types of laws, policies and requirements that exchanging organizations wish to incorporate. Our specific use case includes Title 38, which is similar to 42 CFR part 2, but covers veterans for conditions that go, in addition to alcohol and drug abuse, to include sickle cell anemia, HIV. And we also looked at the Notice of Proposed Rulemaking requirement for withholding information from payers for services that a patient receives, that they have also paid for out of pocket. So, that was another contributing factor to our overall approach.

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

Can I ask a question? This is David McCallie.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Yes, David.

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

It seems what I'm hearing so far is that...maybe I'm hearing a little bit of a mixed story here, but it sounds like the primary drivers are some of these legal technicalities that would determine when a particular part of the record is treated as sensitive. But obviously, in the real world, the patient is going to assume that it had something to do with what they feel about what is sensitive, and if they go and talk about substance abuse with their primary care physician, the patient's not going to consider that that's somehow different from talking to a substance abuse counselor under some technicality of regulatory law. So, is there an assumption that patient has any input into this, or is this strictly driven by need to meet federal requirements.

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

So David, this is Joy. As you probably know, having been in these conversations for years now, this is a really controversial topic as to whether patients should have additional control over their information. We did not want to get into the...dive into the policy controversy in this project. It was primarily designed to enable the implementation of current policy. So, and when an individual does go to one of their providers that are covered by these types of facilities, there is a movement in the administration to incorporate on a more broad basis behavioral health information into primary care provider settings and into their records. We're trying...the focus of this project was to just focus on what existing law...what people have the right to do under existing law and to be able to implement that electronically. Because we see from real wide example that this is becoming a stumbling block for the adoption of electronic health information exchange.

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

...Joy, thank you.

**Walter Suarez, MD, MPH – Kaiser Permanente**

And this is Walter, I just wanted to jump in to mention, I think, from my understanding and the perspective that the... has taken, the idea is that number one, there is law, so there's state and federal law that requires some level of segmentation because some data is treated as specially sensitive by the law. There is the organizational policy which presumably starts with the law and can go beyond the law and give additional rights, if you will, opportunities to the patient to create additional segmentations. And then there is the consumer choice of taking advantage of the law and taking advantage of their inpatient policy and perhaps even going one step farther and requesting additional segmentation as a request, because as we know in the HIPAA, the patient has a right to request restrictions on data. So there are those three levels. I think the approach, while it starts with the law as a way of reflecting what people have organizations have to do, it is expected to be really flexible and scalable to address the three levels I just mentioned. Is that correct Johnathan, I mean from your perspective?

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Exactly right, Walter, and we wanted to start in our use case with one or more policies that were legally enforceable, so that they would be well understood. And we would use that as a basis for exploring the technology and exploring our approach for solving this problem using standards in an interoperable way; and focus not so much on what the policy was, but on how to enforce it and how to make sure that the obligations are enforced on that data as it's exchanged so that the data can flow freely and that consumers would have the confidence that it would be protected properly.

**Stanley M. Huff – Intermountain Healthcare**

And, this is Stan. I'm in agreement with tabling this and assuming the requirement is there. I can't resist pointing out that we have terrible trouble with this because when you implement clinical decision support, and you try and provide the best medical care you can by doing drug-drug interactions and drug allergies and other things. The information is so easily discoverable if you're implementing those things for this protected encounter, it really draws into question whether you're providing better or worse care for the patient based on...if you do the things that you should do in terms of clinical decision support, a person can infer that there was a drug treatment encounter. And if you don't do those things, they you're not providing the best care for the patient. So, it presents a real...so, I'm happy with tabling that, but somehow, I hope we can have...we can get to a policy discussion some other time, because it's really problematic.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

So thanks Stan.

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

This is David again.

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

Stan, this is John Moehrke. I very much echo that, it's not necessarily just a policy problem as well. And it is one of the things that we've spent a lot of time on in the committee, is discussing the almost impossibility of tagging data, especially a persistent tag, that would be able to say this data without a doubt has no relationship to HIV or even that this data is 100% tied to HIV. And then there's the policy side which gives us advanced medical ethics, as you point out, as well. So, absolutely, there's a lot of space to fill there.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Yeah, thanks John. So this is good. As I said in my opening remarks, this is more complex than first meets the eye, and these are some of the challenges that we have been discussing and dealing with. I think that for now the policy discussion it would be good for us to table that and know that we chose one policy that does currently exist and it is difficult to implement for all the reasons that we've just discussed. But, we're keen to try and find a way to enable industry to move forward in the appropriate sharing of data and giving consumers the confidence to know that certain types of data that are currently protected under the law, can have those protections in place in an exchange, in a more granular way. So, that's what we're trying to achieve here. And again, our work is not done, but I think we've made great progress.

And so, just real quick on this slide, before we move on to the next one, in this simplified scenario, in step 2, we have a graphical representation here of the consumer's choices and the data that requires additional protection are captured and recorded. And of course, the patient is informed that the information that they have selected that not be shared, that they're entitled to select that is not shared, will not be shared. So, the little chart there shows that organization A is where all this happens and then in organization B, alcohol, allergies and drugs, so all that information can go to organization B and organization C, the alcohol and drug information is not to be shared. Again, this is just very high-level sort of pictorial representation of some of those potential choices. Next slide please.

All right, so, again on the left hand side now we've got organization A, in the green box or rectangle is organization B. So in step three, a referral requires the protected data to be sent to organization B and because, in the previous slide this disclosure was authorized by the patient, the data that requires heightened protection is sent to organization B, along with the appropriate prohibition on re-disclosure. And in this step, in step four, if we look at organization B's visual representation here, we can see that they have received the alcohol, allergy and drug information, but they are only allowed to share the allergy information, or in other words, the alcohol and drug information carries a prohibition on re-disclosure. And that prohibition on re-disclosure, that obligation, is one of those things that we are trying to enact in our data segmentation for privacy approach. How do we convey that prohibition and have a high level of assurance that the receiving organization will, in fact, be able to enforce it and persist it accordingly.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

I have a question. This is Dixie. On that last slide, you didn't say which end had to be under this 42 CFR part 2 program. It would seem to me the information would be equally sensitive regardless of which end whether 3 or 4 was under that program. Does this cover both cases?

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Scott?

**Scott Weinstein, J.D. – Office of the Chief Privacy Officer, Office of the National Coordinator/ Health and Human Services**

Yes. Because in 42 CFR part 2, not only is the disclosing entity who is the part 2 organization covered by the law, but the law applies to the organization receiving the information, because the sending organization has to let the receiving organization know that this is sensitive, 42 CFR part 2 covered information, that cannot be disclosed without the patient's consent. So, that's what's being shown here. If you see on that alcohol and drugs on organization B side, you see the two yellow triangles, and what that's supposed to signify, again in sort of a high-level way, is a notification that goes along with the data that says, this is sensitive information that you can't re-disclose without patient consent.

**Walter Suarez, MD, MPH – Kaiser Permanente**

This is Walter. Again, I think one of the key elements here is that the...

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

Walt, we can't hear you.

**Walter Suarez, MD, MPH – Kaiser Permanente**

(indiscernible).

**M**

Walter, you're still really muffled.

**Walter Suarez, MD, MPH – Kaiser Permanente**

(indiscernible)...is because there is a federal law that covers all jurisdictions, regardless of which jurisdiction organization B or C are located at. There might be other cases in which the patient might give organization A the request to re-disclose or the authorization I guess, to allow re-disclosure of allergies, but not alcohol and drugs, and then organization B receives that and in that jurisdiction, there might be laws that permit the organization, and this is assuming the data is not again covered by the federal law, but other data that the patient chooses to request not to be re-disclosed, that organization B might not have the requirement to comply with, if you will. And this is following the federal law 42 CFR that covers and protects this type of data, and creates an enforceable portability, the enforceable persistence of a choice made by the patient across jurisdictions. I mean, is that consistent with your understanding Johnathan and Scott and Joy.

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

Walter, this is Joy. I'm sorry but I didn't understand your question. But the reason that we wanted to use 42 CFR as a use case is because it's uniformly applicable, regardless...across the United States, regardless of what state the information is transferred to.

**Walter Suarez, MD, MPH – Kaiser Permanente**

Yes, thanks Joy. I mean the point that I was trying to make is, if this is not alcohol, allergies and drugs protected by 42 CFR, but let's say it's allergies that are not...or drugs that are not covered by 42 CFR and the patient requests that the data to the organization A, requests that the data not be re-disclosed when it's given to the next organization, that next organization might be in a jurisdiction where that data is permitted to be re-disclosed without patient consent.

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

Walter, this is John Moehrke. This kind of touches upon what I said at the top, in that although the minimal use case is solved, was 42 CFR. There is another one as well, but, we also looked at, or at least the standards have looked at much broader use cases, including cases like domestic violence and such that are very much also in the sensitive topic front, but certainly in the need to control front. The second thing I'd like to say on your comment is, it is still incumbent upon the sender to make sure that the receiver can and will uphold any rules that they send to them. So it's not just by simply saying, this data is 42 CFR, I can send it off into the ether, and whoever receives it is bound by the rules. The sender does have a responsibility to make sure that the receiver will abide by the rules that they send along with the data, and that is absolutely a part of the specification we put together.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

Well you and Walter's...the first response I heard actually was responsive to my question and I thought it was clear, and then now you've confused me. Let me ask my question again, just to make sure that...all I asked was, does it matter which end, the sender or the receiver, is covered under 42 CFR part 2? And you guys are answering as if the sender is always that person. If my doctor is sending my record to a doctor who is a 42 CFR part 2 provider, does the rule still apply?

**Scott Weinstein, J.D. – Office of the Chief Privacy Officer, Office of the National Coordinator/ Health and Human Services**

Well if the information is about care received at the non-42 CFR part 2 provider, then that information's not going to be covered information. But once...if it goes to the 42 CFR part 2 provider, and they use it in conjunction with the substance abuse treatment, and the information itself would reveal to another party that the person has received substance abuse treatment, then yes, then that information might become covered by 42 CFR part 2. But the important thing in terms of sender and receiving system in a receiving organization as a non-42 CFR part 2 organization, is that they are...when they receive the part 2 covered information, they are covered...they must keep that information confidential.

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

Dixie, let me approach it in a slightly different way. The way this law works is a little different than many, and what it does is it says, "If the information was originated or maintained by a substance abuse facility that holds itself out as a substance abuse facility and receives federal funds, that's where the protection applies. And then once it applies, it follows the information as it is disclosed. Does that help?"

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

Yeah. But, if my...I think that it's equally sensitive for my doctor to send a message to a 42 CFR part 2 facility, as a referral. I'm being referred over there and they...you know that they're going to include part of my EHR with it...EHR data with it, and those data, to me; and the fact that it's being sent to 42 CFR...a referral is being sent to a 42 CFR provider is equally sensitive as data generated at that facility.

**Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer**

And, as John has stated that when they were considering the use cases here, they wanted to make sure they were extensible to that sort of situation.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

It might be something that Policy Committee might want to take up, because it's clearly a disclosure of sensitive information.

**Scott Weinstein, J.D. – Office of the Chief Privacy Officer, Office of the National Coordinator/ Health and Human Services**

But like we covered, because it tends to reveal treatment at a 42 CFR part 2 institution.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

Right. Right, but the fact that you're referred to there also implies...

**Scott Weinstein, J.D. – Office of the Chief Privacy Officer, Office of the National Coordinator/ Health and Human Services**

Yeah, likely covered, actually, but the law.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

Oh, okay. Okay. Thank you.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

So this is really, really good and you know, I think now we have I think agreement that there is a requirement for data segmentation to exist and there are many different ways and many different policies at the organization, state and federal level, that could invoke such acts of segmentation. And again, what we were trying to do here is pick one as an example of a use case, and actually we picked three and our use case document is pretty comprehensive in explaining the ins and outs of those areas that we analyzed and we know that there are many more. So, the challenge here is, how do we apply this in a way that can be...that can accommodate different policies, different requirements and yet be implemented in a standardized way, knowing that the policy landscape does, in fact, change. And that's what we're sort of trying to focus on.

If we could maybe move forward to the next slide please. And now we're sort of getting into the how. We've seen the why, and we understand that there are requirements for segmentation, and this is a very high-level depiction and we're going to keep going as we get into slide, in some more technical detail. Organization A again on the left, and B on the right. So these are the steps that organization A might need to take in order to segment the data. First of all, they need to identify the information that is further restricted, and be able to recognize that some information is not subject to the policies or the choices that the consumer has made and that some of it is. And then, in step 2 for our example, organization A needs to verify that the patient's privacy consent allows for the disclosure of that protected information and then thirdly, they need to add the privacy metadata to the health information that's going to be disclosed, so that the receiving party knows which information is subject to the special handling requirement.

The converse happens with organization B. When they get the information, organization B needs to be able to process the privacy metadata, associate it with the health information that they received. They need to be able to identify the third party protected information before re-disclosing it and they need to be able to also verify the patient's consent before re-disclosure of the protected health information, certainly in the 42 CFR part 2 scenario. So, that's the sequence and in our next slide, we will focus a little bit more on the how. So, if we could just jump forward one slide please.

As John Moehrke mentioned earlier on, our approach does require that the sending system make the determination that the receiving system is authorized to receive the information before it's sent. And there's also a requirement that the sending system only send the information that the receiving system is authorized to receive. So, this is not an approach that publishes or disseminates information that is somehow redacted or marked as please don't look at this; the onus is on the sending system to determine what can be shared and under what conditions and to verify that the receiving system is able to enforce those obligations, where appropriate. So, for those reasons, we're going to look here at the requirements of the sending system in a little bit more detail. So on the right hand side of this slide, we have a couple of bullet points for each step, that talk about the data segmentation for privacy's mechanism or approach that we think can be used to achieve the process step on the left. And Erik, particularly Erik, please feel free to speak up here.

On the sending system's side, for identifying information that's further restricted, how do we do that? We have the LOINC document type or data type for the CDA, there's the X12 information for healthcare provider and facility types and healthcare coverage site and SNOMED CT for protected diagnoses and problems. So, vocabularies exist that describe information and that can be informative to others, or help the sending system identify information that might be subject to the restrictions. So secondly, verifying the patient's privacy consent. In our implementation guide, we have optional transactions for scenarios involving health information exchange or health information where the sending system doesn't already have a consent in house. So, in those situations, the sending organization might need to query for the location of the consent directive and actually retrieve the consent directive itself.

With the consent directive in hand, the sending organization will be able to check the consent directive and we recommended the use of the HL7 CDA R2 consent directive, and also using the HL7 Purpose of Use Vocabulary, which aligns with the NwHIN exchange for checking obligations. Now, adding the privacy metadata to the health information to be disclosed. We are proposing an approach that uses the HL7 Confidentiality Codes and for the CDA, the codes that are constrained for our use, and I think are constrained in the base standard, are the normal restricted or very restricted values. Also the HL7 Obligation Code to convey an obligation policy such as, a prohibition on re-disclosure without consent, and also the HL7 Purpose of Use. And this could convey the purpose for the information disclosure, for example, to support treatment, payment, operations or research. And we also have a proposed approach that includes a Policy Pointer which is a URL or other XACML Policy Reference. And we'll go into these mechanisms in a little bit more detail, but in the context of responding to the Standards Committee's recommendations on the use of privacy metadata from June, 2011.

#### **Walter Suarez, MD, MPH – Kaiser Permanente**

Johnathan, this is Walter, a quick question on the second level there, the patient verification of a systems...of the consent, it seems to me that there are generally two sources of that; one is the sending organization internally already has a consent that the patient has provided internally, and they already have it documented. Or, there might be an external source where a consent directive that that patient has created is residing, and, is that why these elements are optional, because...

#### **Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

That is correct. Yeah. We recognized that some implementations involving and HIO or HIE would have a centrally or a service or another mechanism to handle the management of consent directives which was out of scope for our use case. We didn't want to get into the mechanics of how consent directive is captured, updated, maintained, revoked and so forth; but what we did need to be able to do is to be able retrieve the sort of fully qualified and enforceable consent directive that had been reconciled and to be able to retrieve that and use the information that it contains.

#### **Walter Suarez, MD, MPH – Kaiser Permanente**

Oh, great, thank you.

#### **Stanley M. Huff – Intermountain Healthcare**

Hi, this is Stan. I have a question, and this borders on the policy thing, so you can throw it off the table again, but I think it's germane to this. I see the use case where for instance what's being exchanged would be a medication list and so there's the possibility now that what you would do is send the medications that are not restricted and not send the medications that are restricted. And it strikes me that that could be clinically dangerous because a clinician...a receiving institution would otherwise assume that this information is complete and so, I guess I'm raising the issue is so have you talked about the fact that you might want to send something with this to say "this list may not be complete," or some indication to the clinician that they can't treat without maybe further talking or some...did that discussion come up?

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Yes Stan, that's a really good question and that discussion did come up on multiple occasions. And what we did not want to do was set policy by defining how to indicate that an incomplete set of data is being sent, for various reasons. You know, that could be revealing in itself as a type of condition that is to be protected and also, I think that there are...it is such a sensitive topic and one that would be determining policy, that we deferred that and would like to receive recommendations on how to handle that kind of default response or provide guidance on that. But in order to do that, we ourselves would need guidance, I think, from the Policy Committee, you know, sending a no response or an indication that the dataset was incomplete or that information had been withheld; there are arguments for and against implementing that type of approach.

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

Johnathan, this is Joy. It's my understanding that in addition to that, you did not get to that, this project is not segmenting at that granular of a level, isn't that correct? You aren't going to...what is being proposed here would not allow, necessarily, the sending of one medication, but not another type of medication. You're not tagging at that data element level, are you?

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

We are not yet, but I think the door is open for that. There are proposed approaches for being able to go more granular. I think Erik, if you want to be able to speak to that please.

**Erik Pupo – DS4P Initiative Harmonization Team Lead, Deloitte Consulting LLP**

Sure, sure and what I would say with that is, there are non-standardized approaches to doing that with different types of patient data. So what we did was, we proposed it as examples for potential piloting, but not endorse or recommend those approaches at this time, until we get some level of feedback as to whether that level of granularity will actually work effectively and can be managed effectively. Because it does have some dangers to it in that it requires a tremendous amount of maintenance at such a granular level for a specific medication or specific procedure or diagnosis.

**Stanley M. Huff – Intermountain Healthcare**

But if you don't get to that level of granularity, I don't see how you even implement a system. I mean, that would just say, it would say, if there were any medications given in the protected encounter, no medications can be sent, which would mean basically, I can't send any...I couldn't send any information to another institution. I mean, I don't see how that even works if you don't have that granularity of information. I mean, I'm okay again with...

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

Stan, it's not really...I mean the point you're bringing up also has a couple of different factors to it. You can absolutely, as a sender, send a short list, you know, not the complete list. It is policy as to whether you inform the recipient as to whether there is missing data there. And of course if you say that, you are indeed indicating that the missing data is probably of a sensitive topic and, gee if you're Betty Ford Clinic, I'm guessing I know what those values are. So, there's absolutely leakage problems around this and those absolutely are often the policy space as to whether you say that you haven't sent everything. What we...what Erik is getting to is, if I send the complete list with specific items in it that should be held to a higher standard of disclosure, maybe it's only a restriction to not re-disclose, you know, items 3 and items 4 out of the list, that's the technology piece that is a gap today. We can't send an allergy list and say item 3 and item 4 have an additional restraint that you cannot re-disclose without giving a consent, which is a requirement of 42 CFR part 2. That's the only piece that's missing.

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

This is David. Can you hear me?

**M**

Yes.

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

I mean I share Stan's concern, I appreciate John's comments, I appreciate how incredibly hard this is, but in reality, the whole point of codifying all these details inside of a CDA is that so systems can pull that data out and do something with it in a semantically, interoperable, meaningful way. So, I don't see how this could ever be made operable without the ability to track at a more granular level. And that brings me to my biggest concern, is I don't see how this could ever be made operable at all, the complexity here and the workflow constraints are so complicated, it's just hard to imagine real-world systems doing this. It works for paper, but this is going to be incredibly hard to build.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

So we have, and I think we've hit on one of the many policy considerations that make this challenging. And if we sort of remove ourselves from trying to, in our workgroup, we removed ourselves from trying to make a determination as to whether the policy was a good policy or a bad policy and what we think the policy should be or couldn't be, we decided to go with what currently existed and to see how far we could get and how granular we could go. What we did do was choose the CDA as our payload for detailed analysis. But again, we also put in considerations where we recognized that not every payload is a CDA and we may have document types or other payloads that don't provide access at that granular level, and we wanted to make sure that our approach afforded an appropriate level of segmentation for documents that weren't specifically structured and semantically coded with inside.

So, yeah, a lot of challenges and again, it's one of those topics that we wanted to take on in order to make some strides and try and figure out just how far we can go with the standards that we've got today, and what would need to change in the standards in order to accommodate a more granular method for applying segmentation. So, I think that there are some work-arounds, but there are some things that can be done and we do have pilots that are stepping forward and willing and able to demonstrate certain capabilities for segmentation, based on our approach. So, I think that is very encouraging and the results of those pilot activities will, of course, be invaluable into figuring out whether our implementation guide is really implementable or not.

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

This is John Moehrke. There is also a method in here that does take care of that fine detailed mechanism, it's just not done at an element level tagging. Essentially you send the unrestricted information in an unrestricted content, and you send the restricted information in a restricted content. And the consumer on the receiving side obviously can import, at will, the unrestricted information and it's only the fine grains that are in the restricted content that have to carry along with it. So ultimately you can do it with a document level control, it just requires you to have two versions of the document which of course gets into the historic definition of the document. If it was a document that was written ten years ago, you cannot change it, it is a document. So, we get into all kinds of those types of stuff; medical ethics, medical records, lots of requirements here.

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

And we have to keep in mind that even though it's technically feasible to do it that way, the workflow burden on the poor provider trying to manage this is just overwhelming, and it just won't happen.

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

Yes David, that's presuming that the doctor actually has to do the work. I don't think the doctor has to do that work that I just explained, that can be completely automated.

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

But then...but now we're treating documents as if they're messages and have semantic meaning of transactions. And by the time these things ping around through multiple HIE stages, that's just going to be almost impossible, isn't it?

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

That's why they're structured and coded. If we're only going to be communicating human to human, we might as well use PDF. So, there's a reason why CDA is structured and coded.

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

But these are CDAs that are structured and coded, but don't have the semantics of transactions and messages. I don't know, if I got that CDA in isolation, that has only the restricted problems in it, how do I know what other problems might be there? Do I take that CDA to say this replaces your current problem list, because there's nothing else in it but these restricted things. Or do I say, well, I'll just add this to the problem list because I don't have any way of knowing what else might be there. And then if it comes in in the reverse sequence, you might reach the completely opposite conclusion. I mean, this is why documents don't work as messages.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

And the other thing that happens if the CDA is kept intact and protected and that CDA as a document continues to be protected as a document, but the doctor may put the information in the problem list or in the drug list separately, at which point it loses the tagging again, right?

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

Right.

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

It should not lose the tagging, that's part of our constraint. If the element has restrictions on it, it has to be maintained with those restrictions. That's very clear to our committee, especially as part of 42 CFR, there is no such thing as decomposing a document, creating a new document without each individual element having its requirement. So that is something that we did discover doing this work.

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

Yeah, this is David. I think...

**Walter Suarez, MD, MPH – Kaiser Permanente**

...I think, this is Walter, I think slides 11 through 15 later on in the presentation, get into a little more of the details of the metadata tagging for privacy and the levels. And, I mean as John points out, there's an approach that is being presented through this S&I framework initiative that at least tries to present a way to address data segmentation through metadata tagging. So my suggestion is, let's let them go through the rest and focus on the privacy section when we get to the privacy section discussion later on.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

Good. Thank you, Walter. Good.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Yeah, next slide please. Okay, so on the receiving system and this is, I think, related to the conversation that was just happening and back to our points earlier, there is an obligation for the sending system to determine whether or not the receiving system is authorized to receive the information in the first place and the receiving system must be able to enforce the requirements that are conveyed. And if those conditions aren't present, then the information would not be sent. So, receiving system requirements; the receiving system must ensure that the provenance of the patient data is tracked, and that will help us determine, for example, if the information came from a facility that has a wing and that wing is a 42 CFR part 2 covered treatment program, then that provenance information would persist. The receiving system must enforce the annotations related to confidentiality, obligations and purpose associated with that health information that they receive from other organizations, in order to prevent unauthorized disclosures. These are some of the receiving system requirements. There are others, but these are the ones that I think are the most pertinent to data segmentation.

Next slide please. All right, we're going to move into the second portion of this presentation now. We've explained at a very high level our approach and we have the implementation guide, which is very detailed that contains much more specific information on which data elements get tagged and what with and at what layer. We start with the CDA, we can apply confidentiality code at the section level of the CDA, at the document header, we can then apply an envelope and then we transport that. And there's metadata that can be attached at various layers in that Russian doll concept. The implementation guide explains that. What we wanted to do was take our implementation guide and present it in a way that shows where we align with the previous recommendations that were made by the Standards Committee, and specifically the Power Team's recommendations on metadata. And so, in order to do that, we came up with, it's not really a stoplight approach, but, those recommendations that we have put a green spot next to, we think we have very strong alignment. Those that have a yellow, there's general alignment with our approach. And those that have the purple blob indicate they're Standards Committee recommendations for which our workgroup proposes alternatives. And then, there were some of those recommendations that were outside of the scope of our initiative and so for completeness, we've included those and just marked them as grayed out.

So, let's go to the next slide please, and talk about...there are a few slides on general recommendations. So, the next slides will follow this similar format. On the left hand side of the table, you'll see the summary of the Standards Committee recommendation and on the right hand side, there will be a summary of the data segmentation for privacy initiatives analysis and response to that recommendation. And in this particular case, we have the yellow blob there on the right hand side, to show that we're in general agreement. And I would just like to say that overall, I think that the approach that the Standards Committee recommended, our approach is very consistent with that. We have some deviation, but generally speaking, we're in alignment. So that's very positive.

So to run through these, and we'll probably need to spend more time on some than on others, but, in this case, the Power Team suggested that metadata for patient identification, provenance and privacy be expressed using elements from the CDA R2 header. In our response, and this is why we've put a general alignment label on this, data segmentation for privacy will use not only the information in the header, but also the IHE XD\* and the XUA metadata to be able to convey the full set of obligations that would be associated with the clinical data that needs to be protected. We reached this decision because the HL7 CDA R2 header is part of the document itself and so, because the header is actually part of the document, it can't be viewed without providing access to the contents of the entire document. And so, this is less of a concern during transit since the data and the metadata is encrypted. It is important for receiving systems to be able to adjudicate the appropriate internal access control request, based on attributes about the data, without having to go actually inside the document itself to find out what is there and what's not there. Okay, if there are no questions...

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

You want questions...responses to these as you go, or do you want us to wait until you do them all?

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Well, I think as we go, but there are some that are related to each other, so we couldn't fit all the recommendations on a slide, so please go ahead and ask your questions and then...

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

Maybe this is premature to ask it, having not seen the rest of them, but, I hate...I'm nervous at the notion of sort of transport specific headers being involved in these complex decisions because we won't always be using these mechanisms of transport or those headers in the future. I mean, we're going to simplify some of that and they'll be just new technologies that won't involve them. So, I mean that's...I would register that as just a potential concern. The second is, I wonder if it's a bit of a false distinction about what the system can and can't look at; you know, kind of by definition the system can look at everything, really the question is what the system displays to the end user under whatever access management is in place to restrict certain information from the user. So, the fact that the system can't read the header of the document without reading the rest of the document seems to be a false constraint, because the system can obviously read the whole thing, otherwise it couldn't process it. It's a question of what they show to the user or what they allow the user to do with it. So anyway, I don't want to get too deep in the weeds too soon, but just register those thoughts.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

And they're good thoughts and actually, I just would like to respond very quickly by saying that our implementation guide does recognize the different architectural choices and exchange mechanisms, you know direct, exchange and others that could be potentially used here to transmit and receive the information. And we tried to be, to the best we could, as agnostic as possible to those architectural choices and as a general principle, we tried to apply the appropriate privacy metadata at the lowest level that was technically feasible, and could be applied in order to achieve the requirements of our use case. So, we started at the payload and we focused on what information was information was in the payload, what information was attached to the payload and then expanded on outwards to the envelope and transport as appropriate.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

So I think, I think you're...this is Dixie. I think you just answered my question, but I want to make sure. I think what you're proposing is that you use XD\* and XUA metadata, but not the context...but not carry the context of the metadata with it, so that you would use these metadata say within a direct message as well, is that right?

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

Metadata exists in a direct message already Dixie. The direct project has already adopted the XCM transport specific version of the metadata. But the metadata is indeed transport agnostic, it has already four bindings to specific transports, one being direct, others being SOAP and a new one that I'm right now working on in HIE which is a RESTful binding. So the metadata is not transport specific.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

Thank you.

**M**

Yeah thanks...

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

The other is a...gives us is that we are then content agnostic. So, for those places who may have created historic data that is only available in PDF form or only available in a previous version of CDA or CCR, but it does need to carry restrictions, this method can carry those restrictions. Indeed, I might argue that maybe we won't be using CDA twenty years from now, so, we may not want to bind our self to content. I think the most intriguing argument I heard just this week was the fact that the CDA documents that might be conveyed, may actually be snapped five years ago. I mean, if we think about doing a transaction ten years from now, it may be communicating a CDA document that was created in some historic past. So, it may not be able to "carry" anything other than what was originally documented. So, there's a lot of positives.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

But I do have...in thinking about it, you said that XDM and XDA are indirect, they are not in the core direct spec...

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

Yes they are Dixie, please take a look...

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

Yeah they are.

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

Please take a look at the direct applicability statements and XDM is absolutely in there, it is mandatory, if the sender can do it.

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

It's not required, it can be used.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

Yeah, that's what I...but it's through the...it's in the applicability statement, it's if you don't require the additional, and this is a question. So you're saying that you don't require that optional ramp, up ramp down piece of...

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

That is only...that's a specification for a service that would convert from one to another. It's not an edge system criteria...

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

Okay.

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

...and yes indeed, the specification says that if a sender has sensitive information, and they need to send that sensitive information, then they do need to support the XDM encapsulation mechanism, I mean, that's criteria that requires them to be able to identify the data; not just confidentiality code, but as provenance, and other factors. So, it's a criteria indeed that is raising the bar on the sender, but it's not adding new criteria to direct. XDM is already a component of direct.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

Okay.

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

Yeah, it is a...this is David. It's an optional component and I think what this...my complexity concerns here raise the question that if this metadata is now essentially required to be, in effect, a part of the communicated content, because without it, you don't know if your allowed to see it, then we have dramatically increased complexity. Maybe that's what we have to do, but, this strikes me as a little bit like you know, sending top secret information around in the government agency and the top stamp is on the envelope, but it's not on the document. And I don't...do it that way.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

We have, yeah, like I said, we have a layered approach here and I think that this is just a general response slide, that we're using the combination of document...combination of tagging at the document level and at the envelope level and at the transport level. And there are multiple ways to assemble the metadata associated with each of those layers in order to achieve segmentation. And I don't think that every implementation will have the exact same way of using that metadata, but the end result should be the same. And again, our implementation guide tries to embrace the wide variation of technical implementation approaches and tries to articulate how segmentation can be achieved using all of these different components and building blocks, where appropriate.

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

But again, complexity issues, are those optional different ways of communicating it or are they required for all messages. I mean, what is the system to do if there may have been message...metadata tagged at a lower level that's lost because you used a different transport protocol. I know it's...I mean, I'll just register that I worry about the complexity. So, I don't want to sidetrack us any further.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Certainly, thank you.

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

David, this is John. As the fact that the document is 200 pages is not because it's complex, we tried very hard to simplify and the optionality that are in here are the optionalities as to whether you as a sender have you know X, Y or Z kind of transport. And actually there's another one that's yet to come for RESTful, but we didn't have the spec yet; I'm working on it. So is MITRE. So a lot of the volume that's in there is just the fact that we had to explain how to do it for direct, because there's the direct project. How to do it for exchange, because there's the exchange product. How do it for RESTful, because people want RESTful solutions. So, it's because we wanted to provide capabilities, not choice, capability and it's not really an option, so to speak, that you are someone who creates sensitive topics. That's a part of your business. So, there's also not...I mean a lot of what may sound like, "well, you could do this or you could do that," the problem is the regulation says you must do this, you must do that. So, there is no choice there, you have to...

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

Yeah, I...first off, I commend you for thinking it through at all those levels of detail, that's awesome work, and I haven't read the document so, I should keep my mouth shut until I read it. But, and I also understand that most of this complexity is actually forced upon us by what I think any sane person would consider to be pretty crazy regulations; you know, the fact that the facility of a certain status determines whether equivalent information has to be protected in one case or unprotected in another case. It's a pretty silly regulation, but, so be it we have it. So I understand all that, but we just have to keep in mind workflow and, I mean exchange as implemented today, really struggles to be useful because of the workflow complexities. And this is going to add to that and it just makes me really nervous that the benefits that we're trying to achieve, without fair exchange will just be that much harder to come by. But, so be it, I mean, I think you guys have done incredible deep thinking on it and hats off to you for that.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Well thank you. And like I said, we still have work to do and the complexity concern is well noted. And I do think it is a complex topic and it's steeped in policy considerations and, we will be carrying forward this implementation guide to reference implementation and pilot. And hopefully we'll have the collective horsepower of our workgroup, along with the results of the pilot to be able to come back and say...at this point in time, this is what we think, but after the pilot, we'll be able to come back and say, this is what we've discovered, this is what we now know. So this is certainly a stepping stone in that process.

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

Thank you.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Why don't we move on to the next slide and this is the second of our general response slides. So, again I think the Standards Committee pointed out here that there were three components necessary to enforce privacy; there was the policy, the metadata about the content and metadata about the requestor. And it goes on to say however, information about the requestor would be used by the sender to mediate the request, but would not need to be tagged onto the data exchanged in an authorized request. It was determined that including the policy, and this is key I think, it was determined that including the policy with each tagged data element was not feasible because policy changes over time. Therefore, it was agreed that a policy pointer to an external policy registry would be the most appropriate. But it was noted that the...I think the Power Team did not address the specifics of how these registries might be implemented.

So our response to that, we looked at possible approaches for sending or pointing to a policy, and clearly we have to be able to do that as a capability within data segmentation, and we focused on two approaches for doing it. So the first, for pointing to a policy, it was determined that the policy reference could be used, and there were various approaches for doing that and we're piloting...we're hoping to pilot some of those, including the use of a policy pointer and the use of XACML encoded policies. And for actually sending a policy, it was determined that the consent directive could be sent to a receiving system and processed, either along with or prior to sending any patient data, so that the receiving system knows what policy restrictions or requirements are placed upon the data that's associated with it. So again here, general alignment, we agree that policy pointers or policy references are important and we have encapsulated that approach within our implementation guide.

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

What does TDE stand for, remind me?

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Yeah, that stands for tagged data elements, and that was a term that I think was originally, or we first started using it in the context of the PICAS report and was used by the Standards Committee's Power Team in that context.

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

Thank you.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Okay, next slide please. So we're going to drill down further here, into the privacy recommendations. So we took the set of privacy provenance and patient identity recommendations from the Power Team's response document and focused on the privacy recommendations as they were the most immediately related to our work. But also those aspects of provenance that were necessary for us to consider, we responded to those as well. So, we'll start with the privacy recommendations. Next slide please.

Okay, so back to the policy pointer topic; the Standards Committee recommendation that a URL that points to the privacy policy, in effect, at the time that the tagged data element is released; and so, in our analysis, we've got the green light here, strong alignment. A policy pointer should point to a universally recognized policy reference to enable their consuming organizations to apply their interpretation of that policy. And I just want to build on that a little bit. There was some concern during our discussions within our workgroup that an organization would potentially be required to consume somebody else's interpretation of that policy. That's not the case in our approach. If we point to 42 CFR part 2 or some other policy, we want that policy to be known and understood, but that the consuming organization be able to apply their interpretation of that policy.

**Scott Weinstein, J.D. – Office of the Chief Privacy Officer, Office of the National Coordinator/ Health and Human Services**

That might include a centralized, some sort of policy bank that the organizations have agreed upon. I think we talked about what Kinetic has been doing.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Absolutely.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

So it's unlikely to be a single policy, right?

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Right, right, unlikely to be. So if you send the information and say this relates to 42 CFR part 2 and Title 38 and some other policy that is specific to the exchange, or that region. Then if I am participating in the exchange and I am able to point to that same, or read from that list of policies, then I would be able to apply my interpretation of what those policies mean, and have my EHR systems automatically apply the rules that are associated with that policy reference.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

So it could be state policies, it could be anything that's in this policy bank, etcetera.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Right.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

Does it take on policy? Like if I send data from California to Tennessee and Tennessee 's privacy policy is stronger than California's, I don't know, so don't...

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

I doubt it.

**M**

The other way around, probably.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

Yeah, that's more likely...

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

Yeah, I'm from Tennessee, I...

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

...moves or does it retain its original...the policy from its original provenance?

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Well, I think we're getting probably beyond the scope of what our particular workgroup analyzed. Clearly if this were to be implemented, there would be more work to be done there, and I don't readily know the answer to that question. I don't know if Joy or Scott wants to hazard an attempt to answer it, but I don't feel that I can.

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

Yeah Dixie, that's...what you're talking about is beyond the scope of this project. There is, however, a SHARP security based project that Mark Frisse is working on out of Vanderbilt, just by chance, and they are looking at exploring policy negoti...computable policy negotiation.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

So with respect to this work, is a policy tagged with its own provenance?

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

Well data is tagged with its own provenance and the recommendation of this work is that any data that is incorporated by a recipient needs to carry the provenance and any restrictions that came with that data. I mean, that became a clear criteria throughout the workgroup. It surprised a lot of us...

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

Say that again John, would you say...

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

...you know, it's not the way that business is practiced today...

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

John?

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

Yeah, run it by us again.

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

John, say that again. That was...that sounded...I missed it the first time.

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

Okay. So one of the conclusions, at least one of the surprising conclusions that I see in this is that in order to support these kinds of data, you know, coming into an organization with restrictions; the organization has to be able to track not only the provenance of the data, which in theory we should all be tracking anyways, but also needs to carry with that data the restrictions that that data came...that came along with that data. No inside your organization is the inside of the black box; how you accomplish that is your organizations criteria. So, we're only going to explain how it comes across, but clearly it became important that a recipient be made aware that it's not just that the document. I mean one example that really kind of brought this to light, and we had some very animated discussions on it is, while I receive a document from you, I only incorporated, 10% of that information into my EHR and ultimately later that day, I created a brand new discharge summary on the patient and I incorporated, in my report, a little bit of that information. That is not a completely unrestricted new document.

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

And that's why; my concern is that this is just a completely unworkable...

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

The regulation that we come from and we were not given purview to change the regulation. So, that's why it is kind of a huge surprise to us. Because everyone says hey, in actual practice, once I've incorporated some knowledge or some information from one document into my EHR, it's now my new document that I created, it's my intellectual property, if you will. And the fact that I incorporated some of your information is just, you know, yeah I'll give you credit for it, but I'm not going to be restricted by it and that was a big surprise when we found out 42 CFR carries that criteria throughout the lifecycle of that piece of information; which means that the tertiary use of my document at the next facility...

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

Yeah tertiary, quaternary...

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

Yeah, that's what I was saying. So it goes...you send that document to somebody else, you add another layer of...another policy pointer, so it looks like you would have an embedded policy pointer within your document as well as a policy pointer...you know, that's what I was asking about tagging the policy pointers with their own provenance.

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

Well I think the third use has to still see the restriction, I don't know if it has to see exactly the restriction as it was written the first time. That's a policy question...

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

And that was a good question. And one of...the obvious example of that kind of restriction would be the prohibition on re-disclosure without consent. So that would need to persist and convey and then receiving organization would need to know that that policy exists, they'd need to know what that policy means and would be able to enforce that prohibition on re-disclosure without going back and getting the consent. And again, that's what we're trying to implement here and I understand it sounds complex and scary, but again, in this use case, please know that we...first of all we weren't discussing really that or trying to discuss the merit of the regulation, but find out whether or not it can be implemented electronically, and indeed we think it can. And we've tried to articulate in our implementation guide, three ways to do that, depending on your architectural station.

**Walter Suarez, MD, MPH – Kaiser Permanente**

And I believe, this is Walter. I believe that one of the next steps, which is already underway, is a pilot. And I understand that the VA specifically is already moving along this same approach of testing and actually implementing this type of technology. Isn't that right Johnathan?

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

That's right. And so I don't know that we can say right now that it's unworkable, but we would have to wait for the results of the pilot to come in to make that determination. And I think one other distinction is that, and this I think is related to provenance and some of the underlying discussion, that in the 42 CFR part 2 use case, not every instance of drug and alcohol abuse would be subject to these privacy restrictions. It would be based on the policy. And if it was a covered 42 CFR part 2 facility, then yes, that would make it subject to the restrictions. But if the health information exchange had a policy that allowed patients to make those choices and the organization participating in the exchange agreed that that was a policy that should be offered to the consumers, and were a legally valid policy, then sure, why not.

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

Well, but if...this is David. I mean, if a single instance of this ever has to occur, then all systems have to support it, so, the fact that some data isn't restricted this way is kind of moot. The question is, is it ever needed and if it is ever needed, then all the systems inherit the complexity.

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

Well, only the systems that are being communicated to.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Right and if...

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

If you're asking for data and your system can't support this, then I can't send it to you.

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

Well, but now my system has to understand that this is the question that has to be asked and you have to understand that I can't support it. I mean again, there's a...if all this is supposed to happen automatically in the background, then these negotiations have to be understood by software. So...

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

Yeah, but we're building on...

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

I mean, my point is that it's optionality, you know "or" means "and" in our Standards Committee mantra, so. But I wanted to shift back to a slightly prior question which is, does...is the assumption that these policies are computable a part of your working model? I mean, in other words, is the downstream systems, are they supposed to chain back the policy pointers and presumably execute and understand the XACML and enforce the rules, or...I didn't follow whether your assumption is that these are computable policy enforcements.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Well, I think to the extent that the organization wants to be able to act on them in an automated way they would have to be. But I don't think that they would be...the receiving organization would be receiving necessarily the XACML format of the policy; they might have their own. But they might use the standard or a list of well-known policies to know which XACML rule set to apply, within their organization.

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

Right.

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

Is there any place where that's been done at any meaningful scale? I mean inside healthcare, outside healthcare. I know there are pilots that show it, but...

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

Well, yeah, I just want to add a clarification is this does not require computability at the definition that one would see in XACML. What it requires is computability that if I see the vocabulary item that says, "Do not re-disclose without further consent," that I understand the meaning of that vocabulary. And that concept is absolutely the whole concept as to why LOINC works, why SNOMED works and why...every single vocabulary within healthcare has a meaning behind a vocabulary item. So, it's nothing new from that perspective. We absolutely all know what computing process is needed by a laboratory when they receive a request for a CBC.

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

Right, John. I understand that. John, I understand that. The question, I mean, if it were possible with simple standardly agreed upon codes to communicate sufficient policy that a downstream system could look at the code and know what the policy is, then we don't need XACML ever. But your model is implying that you need XACML, which is, if you would, a post-coordination of policies that now require not only agreement on the meaning of those codes, but an agreement on certain rules and rule rubrics and so forth, to understand how those codes in combination affect some more restrictive or more complex or more subtle policy. And so if you're saying it can be reduced to a simple code set, I like that, but I'm not sure I hear that, right. I'm hearing something that's much more complicated than a code set.

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

Well yeah, some things can, and we're working on a set of vocabularies that fall within the access control concept of obligations, which is that you must do X. We're working on vocabularies in the security concept domain of a...what's the other one...I want to say promise, but it's not promise, it's...

**M**

Purpose of use...

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

No...well purpose of use...

**M**

Are you talking about some of the refrain policy?

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

Yeah, the refrain policy. That's the word I was looking for. So there is...where these things can be policy atoms, we will create vocabulary for them...speaking again here, just now, as the HL7 Security Workgroup co-chair, we're working on those right know...couldn't leverage them because they don't exist yet, but they're certainly identified. But absolutely, policy could go beyond that vocabulary in the same way that a new laboratory request could go beyond LOINC, right, and you deal with that. And XACML is one way to deal with that. Another way to deal with that is locally negotiated...just like you do with lab.

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

And I'm...I would register my concern that the complexity of XACML is just way beyond what we'll see implementable at scale. I mean, we have trouble still to this day figuring out how to communicate "allergy to latex." I mean literally, we still don't know how to do that. The thought of communicating complex policies that require kind of nationwide understanding of a rules model is just, and to me, it just doesn't seem likely. So, the degree to which we can focus the minimum requirement under these arcane laws into code sets which everyone understands, boy that seems like worth pursuing, because I don't think you're going to do it with the more complex approaches.

**M**

(Multiple people, all talking).

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

...here is that we should be able to reference the policy and allow the consuming organization to apply their interpretation of that policy rather than someone else's. So, I'm not going to try and force my understanding of 42 CFR part 2 on another organization.

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

By the way David, I totally second your concern there. I too would like to see policy fragments identified as well understood vocabulary items. And, by the way XACML needs those as well, because XACML doesn't have fundamental...I mean, it doesn't have a vocabulary, it just has rules, you know, "if," "then," "else" -- it's just a language. So it needs a vocabulary, so we need to provide vocabulary in both cases, but I agree with you that XACML is a very difficult thing to process.

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

Yeah, I totally agree. I mean, XACML is just...is a rules engine, but it's empty otherwise and you have to have all of that stuff and pre-agreement. It's worse than post-coordination because it's more flexible than post coordination. Can I ask one question?

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

No question. It's more similar to drools.

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

Yeah, exactly. And drools would be a better choice, frankly, but that's another debate. One question I wanted to ask Joy, if she's still on, or anyone who's actually our policy expert, and that is, does the patient's consent trump the 42 CFR constraints? In other words, if the patient who has gone to a 42 CFR facility, when the encounter is over, happen to say, "I want you to share my sensitive information with everyone, I place no constraints on it," would that release the 42 CFR organization from having to apply all these rules, or does the law trump the patient's wishes and say "too bad, I still have to put all these restrictions on it."

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

The way that the regulation is drafted is that the consent to disclose has to be...it can't be just a blanket consent, it has to specify the recipient. And it doesn't have to necessarily be to Dr. Smith, it could be to a hospital system, it could be to "all of my healthcare providers," well, probably not that wide either. But it has to be more specific that I'm going to share it with...because of the requirements of the consent form are specified in the regulation.

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

Okay, so they can't really completely waive their...they can't waive these rights.

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

That is correct.

**Scott Weinstein, J.D. – Office of the Chief Privacy Officer, Office of the National Coordinator/ Health and Human Services**

And even when the information is sent with the cons...in accordance with the consent, when it gets to that consented party, the prohibition on re-disclosure still applies to that party.

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

Yeah. So what I'm...I mean, so I'm thinking you know radical simplification here or an inversion of the problem and wondering if maybe this data from these incredibly complicated regulatorily constrained systems never flow into the rest of the world, but can only be accessed on demand with consent, in the presence of the patient. I mean, are we making a mistake to assume this data is flowing, maybe it should never flow, it should only be pulled on demand?

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

Well it's already flowing in some real live context.

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

Well maybe it shouldn't be, because I don't think we're going to be able to handle it in the next five years.

**John Moehrke – Health Information Technology Standards Panel (HITSP)**

Yeah David, my understanding from the introduction we were given is that it is either A – flowing with no controls or B – not flowing because there isn't ability to flow and the concern was both cases were bad and the B case, there was a desire to, "can you guys figure out a way to get this to flow." So, that's essentially our charge, was can you figure out a way to get this to flow with these restrictions. The other thing I's like to...was you mentioned earlier, by the way, for example within the NwHIN exchange, the DURSA already forbids any data that flows through the NwHIN exchange to be re-disclosed without a new consent. So, what they did there was they said, this rule is good enough for all data. So, it doesn't have to only go on 42 CFR part 2 data, it's on every data.

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

Well, and I kind of think that's the logical conclusion of this is it should either apply to everything or it should be so carefully walled off because of its special legal constraint, that it's clear that it only applies to these specially walled off things. This kind of mixed world where is you tell your primary care physician that you have an alcohol problem, he can re-disclose that freely. But if you tell a substance abuse provider who receives federal funds that exact same story, he can't disclose it freely and that every subsequent exchange downstream has to remember and respect the difference between those two circumstances, which is a complete artifact of where you got care; we'll never have systems that work at scale or operate smoothly. That's just crazy.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Well, if I could just jump back in here, and I'm looking at the clock, this one slide was actually a slide where we did have agreement with the Standards Committee recommendation for that use of policy pointers. Again, we were not trying to, and I certainly appreciate the concerns about the complexity of the policies and how they can be implemented in a scalable fashion, that's what we're trying to investigate and that's what we're trying to do. So I think that it would be probably useful to defer the conclusion until we have the results of the pilot, because there are members of our workgroup that believe that this can be done. And we'd like to be able to demonstrate that it can be done, so that they can then share the lessons learned through that pilot process back, and we can update our implementation guide and certainly report back on what worked and what didn't work, at the completion of the pilot phase.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

You know the VA pilot that you mentioned earlier has been going on for several years at this point, maybe approaching five years. Did you get testimony from Mike Davis and his team down there on what worked and what didn't work?

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Yeah, absolutely. And in fact, Mike Davis and his team are considerable contributors to this body of knowledge in our workgroup, a regular participant and they have come forward as the pilot that our community has endorsed to test this approach. And so, they are going to be building in the capability to enforce these prohibitions on re-disclosure as another policy attribute, into their system that they have been working on and building for the last few years. So, this capability is going to be included within that pilot activity.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

Okay, thank you.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

So, I don't know Dixie if we're going to be able to get through all of these slides. Would you like me to just...

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

Why don't you just move ahead and let's try to get through the slides and everyone, please...this obviously is a topic that we're all very interested in. So again, thank you, but let's just charge ahead and go through the rest of the slides and let Jon complete the slides and then use whatever time we have before public testimony to ask any additional questions.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Yeah, thank you. If we could just jump forward please, and I'm just going to touch very, very briefly here, and focus on those areas where we're proposing an alternative approach or did not have strong alignment. Those areas that we did agree with the Standards Committee recommendations and have incorporated that into our approach we can probably just gloss over. So, sensitivity is one area that we're proposing an alternative approach. So, the Standards Committee recommended that metadata pertaining to privacy include the content metadata of data type and sensitivity, we agreed with the data type. For sensitivity, indicating special handling that may be necessary per the reference policy. That was the Standards Committee's recommendation.

In our approach, we actually ended up being less granular in the sort of word to word interpretation of that recommendation. We're approaching to leverage the confidentiality codes, which have a constrained value set within the CDA of normal, restricted or very restricted, and it would be our recommendation that data that has 42 CFR part 2 relevance be marked as restricted. Data that is marked as very restricted probably would be pulled out of the exchange or is not currently included within the scope of our use case. And data that would be marked as normal would not be subject to the enhanced protection that's required by law. So, there's another slide that talks more to this, but the bottom line here is, the original recommendation from the Standards Committee on sensitivity, we're recommending that we move forward with the HL7 Confidentiality Codes as the initial way of marking the data as having a restriction.

Next slide please. So building on that, the Standards Committee recommendation to extend or expand the HL7 vocabulary for sensitivity includes a proposed starter set, such as substance abuse, mental health, violence, genetic information and so on. Again, we thought that including that type of information in the document header was revealing and we think that using the HL7 Confidentiality Code vocabulary with a constrained value set, is our approach. And the rationale for that, those sensitivity codes are used as a shorthand reference to the privacy policy that deals with them, and that sort of, I think, there's a correlation there between this proposed value set or starter set, to the catalog of policies that we talked about earlier. Enumerating these policies in a code set is not fully scalable. We know that policies evolve and new privacy policies are introduced over time and initially this would have to be extended to include sickle cell anemia, sexually transmitted diseases and would require constant updates. The detailed sensitivity codes also only really have true value when used in the context of the privacy policy; so labeling something with a substance abuse sensitivity code is useful when we know how to handle the data that is associated with that label, and so the policy becomes important. The sensitivity code by itself is somewhat redundant. The sensitivity code by itself could indicate that it was restricted information, so why not just say this information is restricted and then use the policy pointer that the Standards Committee recommended, to communicate how that restriction would be implemented. Okay, next slide please.

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

So, can I ask a question there?

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

No, we want to just let him move ahead David, write it down and be prepared at the end.

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

Okay. I mean I agree with...

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

We can skip over this slide, we have agreement with the Standards Committee recommendation for data type and LOINC codes, so, next slide please. Okay, so the provenance recommendations, again, we were focusing on privacy to the extent that provenance was not analyzed to define specific guidelines, but does have an impact on how data segmentation approach works and we've responded where we felt we could. So, next slide please. General alignment, metadata contained within the provenance envelope should contain the tagged data element identifier and that other information. So, that metadata is included within several components of the data segmentation approach, and we recommend that metadata that defines provenance is established at the document level or the payload level, wherever possible, allowing the specific attributes inside the document to show they're in provenance in the context of that document. But because the payload mechanism may support alternative formats such as DICOM, X12 and there are many other types of payload that don't readily lend themselves, and provenance for those formats may differ significantly from the way that we've described in our implementation guide. So again, we're agreeing, but we're recognizing that other types of payload will still need to flow.

Next slide please. We've got general alignment with the use of certificates and the use of digital signatures was not specifically addressed by our initiative. We've got preconditions and assumptions related to mutual authentication and the other security attributes associated with implementation of digital certificates and digital signatures. Next slide please. This is another slide on the use of X.509 for digitally signing envelope contents, and again, we didn't have a specific recommendation here, but our assumption is that those recommendations are consistent with what we would be handling through assumptions. Next slide please. The actors and actor's affiliation are expressed within the 509 certificate and the recommendation from the Standards Committee to include additional optional metadata fields; we also added the following requirement. We agreed with that, but we added the requirement that the receiving system must be able to ensure that the provenance of the patient data is tracked for the purposes of being able to fulfill the requirements in our use case, as currently written in the existing regulation. Next slide please. Yeah, the last one on provenance again, we had no strong opinion on and didn't address specifically. We included it in this deck for completeness.

Next slide please. Our privacy recommendations...

**Scott Weinstein, J.D. – Office of the Chief Privacy Officer, Office of the National Coordinator/ Health and Human Services**

I think John, it is a typo. We're now going into the patient identity recommendations.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Thank you. Thank you, Scott. Yeah, for patient identification again, the attributes that we addressed here were not specific, we looked at them in the context of data segmentation, but didn't look at the Standards Committee recommendations line by line with a purview of responding to them. We responded to those that were pertinent to our workgroups activities. And there are just a couple here. So, next slide please. Extending HL7 id element to allow a URI to be used. That recommendation was out of the scope for our workgroup, and most of these patient identity ones were. Go ahead, next slide please. The metadata pertaining to patient identity should include the following, and there's a list of items there. We did cover those data elements within our analysis and determined that the metadata for patient identity should primarily be concentrated in the metadata associated with a name, ID or organization and within the patient data itself for anything else such as the zip code or data of birth. And just sort of anecdotally here, one of the overriding preconditions to be able to exchange data that requires enhanced protection under the law, that we have positively identified the subject of that data. So, we know who the patient is before our exchanges occur, so the PIX PDQ or other cross-referencing or patient identification mechanisms were indeed prerequisite activities to the implementation of our use case approach.

Next slide please. And we can move one more slide. Erik, would you talk to this one real quick please, it talks a little bit about our approach as it relates to direct.

**Erik Pupo – DS4P Initiative Harmonization Team Lead, Deloitte Consulting LLP**

Sure, sure. So, as John Moehrke mentioned, the use of IHE XDM was already recommended, which you need to run...statement. As part of our implementation guide, we did do an analysis of SMTP/SMIME and did not think that it can support the explicit definition of a lot of the metadata that we talked about within this initiative. So, we basically recommended the usage of XDM to support that metadata, and then also recommended alignment with the Direct XDR and XDM specifications also available through the direct project, to allow for the bridging between direct environments and exchange environments. So, if a sending system is using direct and that is being sent through an HIE, the use of that specification would be used in support of that goal objective.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Thanks Erik. On our last slide, the next slide, we do have a reference here to the white paper that was written by Melissa Goldstein and Scott Weinstein, who's on the call here from ONC contributed significantly to that. And it explains and discusses the policy considerations and analysis that we talked about a lot today on this call and some of the reasons behind why segmentation is important and necessary. And again, our approach here is to try and find a way to determine actually, if this information, this data, that requires special handling under the law can flow more freely, while affording the consumer, the patient, the appropriate protections that should be in place. So, it is a difficult challenge and one that we have been working on since October.

We have now gotten to the point where our implementation guide is just about ready for pilot implementation, we've identified a pilot and again, our workgroup consists of over 150 members, 50 committed member organizations and we have between 30 and 50 people attending our calls, up to three times, four times a week sometimes for several hours. So there's a considerable amount of work that the community has put into articulating our approach and we do feel that despite the complexities of the regulation and the complexities of having different policies and architectural choices, that this is an achievable goal and one that we look forward to testing more fully through the pilot activities and then having the opportunity to report back on our lessons learned there. I'm sorry for rushing through those slides so quickly at the end, Dixie, Walter and members of the workgroup, but that's the end of our presentation.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

Thank you very much Johnathan and Scott. This obviously represents a lot of really tough, hard work and a lot of hours put in and we really appreciate the effort and we appreciate your taking the time to present it to us. So David, would you like to ask your question?

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

Yeah, well, it was a comment really more that I agree strongly with the notion that sensitive information should be flagged with a marker in some way that indicates special handling is needed. And maybe even codify to what degree special handling is needed, but it should not be flagged with what's in it that makes it need the special handling. I think that makes a ton of sense, you don't want to enumerate all of the reasons why this information is not to be exposed, because you just exposed it by enumerating why it's not to be exposed. Just mark it special handling required. So, I like that, that makes tons of sense. I am, I'll just register again my overall concern about complexity obviously. The other concern is this layering of metadata and payload and transport specific...the need to get transport specific about how that stuff is flagged is going to be a problem in the future, I think. And then my final comment is, way back at the beginning I think, the notion that coded data is going to get teased out and out of its payload even and put into problem lists and medication profiles, and things like that, at which point it's granular information. And so we can't ignore the fact that if that granular information somehow has to obey these special rules, that we're going to have to track this at a level of granularity way beyond what we're currently doing. So, that's another concern for the future.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

This is really good feedback and very timely, because like I said, we haven't gone into pilot yet, we're embarking on the pilot phase and implementation guide, while it's going through consensus hasn't been published yet as final. And so, we very much appreciate these comments and we'd like to take them back to our workgroup for discussion, so that we can make sure that those concerns are indeed registered with the implementation guide and discussed there.

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

And despite the critical sounding nature of my comments, I have incredible respect for the hard work that you guys have done, it's just overwhelming. So, much appreciated.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Thank you.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

I have a question about some of the special types of sensitive information, like sexually transmitted diseases is one that comes to mind, also are reportable to public health, and HIPAA really sort of...it doesn't exempt public health by any means, but it doesn't put public health exchanges under the same restrictions as other information. Have you discussed how that might work, like, if you're reporting a sexually transmitted disease, gonorrhea, syphilis to CDC, do you still tag it, or is that an exception or how does that happen?

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Well thanks Dixie, that's a great question and actually Walter might be best able to answer that for us. But I think that if our policy allows that information to be sent, it does get sent, obviously, but as to whether or not it still gets marked as having a tag or prohibition on re-disclosure, I don't know the answer to that. Walter, do you have a sense of what should happen there? I don't know if Walter is still on, Joy or Scott, if you have a thought there. But Dixie, I don't know the answer to that.

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

The public health laws are very state specific and many of the laws that prohibit the re-disclosure of, for example, HIV information, are directed primarily not at the provider, but at a public health entity. So, it raises a...it's an interesting question Dixie. It raises a whole other perspective on how you would approach this, because marking something with a policy tag as has been proposed, might actually be very helpful for the public health organization, because it could then go and say, "oh, this is information covered by X," under that law, we are restricted on how we can deal with it, like we can use it for certain reasons, but not for others.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

And I thank you Joy, I appreciate that. It's not something that we've discussed at length Dixie within our workgroup, but it's an interesting look at things that we should probably discuss and also...

**Erik Pupo – DS4P Initiative Harmonization Team Lead, Deloitte Consulting LLP**

Johnathan, I can answer that by just saying that in work through the CDC for things like healthcare acquired infections and the reporting associated there, this method actually would work there as well, because their method of reporting right now is CDA-based and they would be able to support the use of the confidentiality codes, if need be, for something like a sexually transmitted infection.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Thanks Erik.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

Even though the policy at the other end would be different, the method of getting it there...the rules for getting it there would be the same, in other words.

**Erik Pupo – DS4P Initiative Harmonization Team Lead, Deloitte Consulting LLP**

Yes.

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

Okay. Are there other questions? Okay, why don't we open this up for public comment, we're...I assume it's over 8, actually 8:01 have. So, MacKenzie, would you just op...

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

Sure. Operator, can you please open the lines for public comment.

## **Public Comment**

**Caitlin Collins – Altarum Institute**

Yes. If you are on the phone and would like to make a public comment, please press \*1 at this time. If you are listening via your computer speakers you may dial 1-877-705-2976 and press \*1 to be placed in the comment queue. We do not have any comment at this time

**Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences**

All right, well thank you all again. We really appreciate the hard work and your taking the time to present it. Thank you Joy for setting this up and if anybody has further comments that they'd like to convey, certainly feel free to follow up with Johnathan or through Walter, however you want to do it. Walter, would you like to say anything more? Oh, he's not there, that's right. Okay, thank you, have a good weekend everyone. Bye bye.

**Johnathan Coleman – Office of the National Coordinator – Initiative Coordinator, Data Segmentation for Privacy**

Thank you very much.