

**HIT Policy Committee
Privacy & Security Tiger Team
Transcript
March 10, 2014**

Presentation

Operator

Thank you. All lines are now bridged.

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

Thank you. Good afternoon everyone, this is Michelle Consolazio with the Office of the National Coordinator. This is a meeting of the Health IT Policy Committee's Privacy and Security Tiger Team. This is a public call and there will be time for public comment at the end of the call. As a reminder, please state your name before speaking as this meeting is being transcribed and recorded. I'll now take roll. Deven McGraw?

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Here.

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

Hi, Deven. Micky Tripathi?

Micky Tripathi, PhD – President and Chief Executive Officer – Massachusetts eHealth Collaborative

Here.

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

Hi, Micky. Andrea Wilson? David Kotz? David McCallie?

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

Here.

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

Hi, David. Dixie Baker?

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

I'm here.

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

Hi, Dixie. Gayle Harrell? John Houston? Judy Faulkner?

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems Corporation

Here.

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

Hi, Judy. Kathryn Marchesini from ONC?

Kathryn Marchesini, JD – Policy Analyst – Office of the National Coordinator for Health Information Technology

Here.

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

Joy Pritts from ONC?

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

Here.

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

Kitt Winter?

Kitt Winter – Director, Health IT Program Office – Social Security Administration

Here.

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

Larry Garber?

Lawrence Garber, MD – Internist/Medical Director for Informatics – Reliant Medical Group

Here.

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

Hi, Larry. Leslie Francis? Wes Rishel?

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Here.

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

Hi, Wes. Stephania Griffin from the VA?

Stephania Griffin, RHIA, CIPP, CIPP/G – Director, Information Access & Privacy Office – Veterans Health Administration

Here.

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

And welcome. And are there any other members from OCR on the line? Any other ONC members on the line? Okay, with that, I'll turn it back to you Deven.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Great, thank you very much Michelle. Uh oh, I have an echo. Do you guys hear an echo on my end?

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

I think it stopped.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Okay, great. So what we're going to cover today are first want to introduce a couple of new participants on the Tiger Team. I want to make sure that all of you have knowledge about an upcoming hearing that Dixie's Health IT Standards Committee Privacy and Security Working Group is having on NSTIC. We're going to move to finalize our presentation to the Health IT Policy Committee on access to adult patient view, download and transmit account.

And then we're going to move to discussing a new bit of work that we're being asked to do by the Certification and Adoption Workgroup that relates to the data segmentation for privacy work – the pilot work that's been going on with ONC. And so I suspect that most of our call will involve a briefing from someone who's been very involved with that pilot, so we can understand what the outcome of that was and then we'll continue on with discussion of that on our next Tiger Team call. So, it's a pretty packed agenda today, but an interesting one.

So I want to first start off by introducing two new ex-officio members of our Tiger Team, who come from the Veterans Administration. Stephania Griffin, who is the Director of the Information Access & Privacy Office and Andrea Wilson, who I heard on roll call here with us today, which is great, who is the Veterans Health Administration Privacy Officer in charge of HIG, she can tell us what that acronym means, Information Access and Privacy. So Andrea, welcome. You're on. I didn't hear Stephania's name being called, but I certainly don't want to leave her off if she is also on.

Stephania Griffin, RHIA, CIPP, CIPP/G – Director, Information Access & Privacy Office – Veterans Health Administration

Hi, this is Stephania Griffin, actually, Andrea Wilson is not on the call –

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

– I reversed it, I'm so sorry. Well Stephania, welcome. We're eager to have both of you participate, I think it will greatly enrich our – the level of experience on the call and our discussion. So thank you, very much. Okay, now just wanting to make sure that all of you are aware of the public hearing that the Health IT Standards Committee Privacy and Security Workgroup is having on the National Strategy for Trusted Identities in Cyberspace. It's coming up this week, on March 12; there's a link for more details. I know that I received an invitation to participate in this if we wanted to, Dixie, do you want to say anything more about this?

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

Perhaps just that the – because I have been asked, what do you expect to be the outcome? The real purpose of this public hearing is to really gain a realistic and objective view of where the NSTIC – what NSTIC is, what it's intended to do and what – where it currently stands. So we hope by the end of this hearing that we'll have a much better understanding about its potential for really use in healthcare.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Well, that's great, I'll definitely be – I think we would definitely be interested, those of us who are not able to participate in the hearing, hearing from you on a future call about how it went. Because so many of our previous recommendations on identity proofing and authentication of both providers and patients left room for the development of nationally adopted standards or options for a reusable, high-assurance credential that might come out of the NSTIC process. So this is really exciting and thank you for inviting a broader array of folks to sit at the table for that.

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

Sure, and we'd be happy to report back.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Great. Thank you. Okay. So we circulated the – our recommendations related to view, download and transmit access to – for adult patients by friends and family designated by the patient or by a legal personal representative. And what we asked you to do when we circulated those documents was to provide us with any additional language changes. And we received two suggestions; one was to be clear on slide 5, for those of you who are following along on paper, was an addition of making clear that the education of patients and providers be both about rights and responsibilities and any potential limitations to the capability. That was suggested language from John Houston. And then on the next slide, it was just a tiny wordsmithing change around educating patients about concerns for VDT access when they enable that by sharing their own passwords. And really this change was quite small, we had put – the original slide said some education and now it says education and so just makes clear that there needs to be education of patients along these lines, but without a whole lot of detail on what that...

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

Deven, you've gone offline.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Oh. I have, you can't hear me?

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

Now we can.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Oh, okay. So sorry, was just explaining that change, at what point did I drop off? I was probably rambling anyway.

Micky Tripathi, PhD – President and Chief Executive Officer – Massachusetts eHealth Collaborative

It was just the last piece, you –

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Can you hear me now? I picked – I just picked up my speakerphone, can you hear me?

Micky Tripathi, PhD – President and Chief Executive Officer – Massachusetts eHealth Collaborative

Yeah, I think you were – Deven, I think you were basically done. I think you were just saying that the prior version said some education and now it says education to make it clearer.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Yes. Thank you, much better stated, succinctly. Does anybody have any issues with either one of those changes? Okay, terrific, so we'll finalize those recommendations and move to – and present them – the other recommendations where there were no changes to what was sent to you are in the backup slides. And we will be aiming to present those recommendations to the Policy Committee at their April meeting, because we don't have room on the agenda to present them tomorrow. All right, terrific.

So with that, we'll move into our next topic for today and it starts with a slide that comes to us from the Certification and Adoption Workgroup, which has been looking into the issue of a voluntary certification process for behavioral health providers and long-term care providers. And they have been investigating the set of issues that would – the set of technology capabilities that would need to be present in such a voluntary certification program. Again, it's voluntary because those providers are not eligible for Meaningful Use incentives, and so – but it would be incredibly helpful from a coordination of care standpoint if there were interoperability among the EHRs that are used by that population of healthcare providers and the population of providers who, in fact, are eligible for subsidies.

And the Certification and Adoption Workgroup recognized that particularly with respect to behavioral health providers, that there would be a need for those providers to be able to transmit information in a way that was compliant with the additional privacy and security requirements that a number of behavioral healthcare providers have to abide by, that apply to federally funded substance abuse treatment programs. And what the Certification and Adoption Workgroup essentially said was that yes we recognize that these requirements are – apply to behavioral health providers. But because those requirements also include what are called redisclosure provisions, meaning that once the information has been shared with another care provider, there still are additional consent requirements that may attach to that information shared from the behavioral healthcare provider for subsequent disclosure. That it really made sense for any technical capacity that would be built in to behavioral health's provider certification, also potentially be part of certification for other providers, too, in order to avoid creating more of a siloed situation where the behavioral healthcare providers can share the information, but the other care providers may not have the capacity to do so.

And so essentially, what they've requested is that we examine what's been proposed for the standards for protecting the privacy and security of this data that is subject to more stringent federal requirements. And that triggers a need for us to understand a bit better where the data segmentation for privacy pilots have landed and what that technology looks like from a policy standpoint. And so we're going to have a presentation on that, but before we move to that Joy, I know that you wanted to lay some foundation for this discussion as well.

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

Right. So we've had the discussions on this issue before, but I think it worth our time to just go over a little bit about what is at play, in particular with behavioral health. So, as many of you know from prior discussions, there are federal confidentiality regulations that apply to certain behavioral healthcare providers. And those regulations require those healthcare providers who are subject to what we have often referred to by its citation as 42 CFR Part 2, that providers who are subject to the 42 CFR Part 2 requirements must obtain patient consent before they disclose their health information to most other – in most other context. There is, of course, an exception for medical emergency. But where HIPAA would allow a provider – most providers to share health information for treatment purposes, for example, without the patient's permission, 42 CFR Part 2 actually requires the patient permission to share it for that purpose.

When a provider does obtain a patient's consent to share that information with another, they must accompany the disclosure with a notice that informs the receiving party that the information has been disclosed from records protected by these higher federal standards. And that the information may not be further disclosed unless expressly permitted by the written consent of the person to whom the information applies – the subject of the information. So there are two, I think, really – what we've heard as the two key challenges here in implementing this electronically, have been communicating the – have been identifying that the information is protected by 42 CFR Part 2 and providing the notice to the receiving party that they may not further disclose it.

So we're not here today to discuss whether people really agree or disagree with those standards – this regulation. It is in place and we have been attempting to find ways to help providers actually electron – be able to electronically comply with this law, so that the behavioral health community is not excluded from the benefits of health information exchange. And that is pretty much the genesis of the Data Segmentation for Privacy Project and I think that it would be a good time now to turn it over to Johnathan, to explain – to give a little explanation of where that project has been.

I think before I get to him to give the update, the – I'll give a very general overview that that Data Segmentation for Privacy Initiative was run out of the S&I Framework Initiative here at ONC. And had a number of private stakeholders involved and it has now been, I'm trying to think, Johnathan will be able to tell you better as to how long it's been going on. But, this is the Initiative that really kind of ties our effort to ensure that behavioral health providers are included in health information exchange, the policy to the technology. Johnathan?

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal - Security Risk Solutions, Inc.

Yeah, thank you very much Joy, I appreciate that. And thank you to Deven and Micky and members of the Tiger Team for having me on today. So, as Joy said, the Data Segmentation for Privacy Initiative at ONC has been going on actually for over two years now, including a full year of testing and implementation and validation in some of the pilots. And I'll talk to – briefly talk to some of their successes as well, as we go through the presentation. So, I think to get started, if you could – do you want me to just announce when to maybe move on to the next slide?

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Yeah, yes, that – because Altarum will run your slides for you Johnathan. I thought they were just – they're pulling them up I think now. Okay, yeah – not those slides, the Data Segmentation Update slide deck. Just give us a minute to pull them up. This is a separate deck.

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

Yeah, no problem. Thank you.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Yeah. Are we start...?

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

Altarum, can you just – okay, there we go.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Thank you. Does that look like your deck, Johnathan?

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

Yes it does, thanks so much. And we can advance past the title slide, if you like, and I can – if there are no other I guess questions up front, I can dive into the meat of it here.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Go right ahead, Johnathan.

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

Okay, thanks so much. So I'm just going to start with a very brief, two-slide user story example to sort of build on the scenario that Joy laid out. So in – and I know some of you have seen this before, but I think it serves as a useful refresher just to see how and where the data segmentation standards come into play. So in this scenario, a patient receives care at their local hospital for a variety of conditions and in this scenario, it includes substance abuse as part of a covered Alcohol/Drug and Abuse Treatment Program. And so in Step 2, their still within their organization and there is data that requires additional protection, and so the patient's consent is captured and recorded, and of course the patient is advised that the protected information won't be shared without their consent.

So this is a Step 1 of our use case, provider healthcare organization number 1, as shown in the big blue rectangle and you can see on that sort of representative chart in the diagram, that organizations number 2 and 3 are listed. And again, this is just purely so you get the gist of it, organization number 2 has got a green checkmark next to alcohol, allergies and drugs and organization number 3 has not been consented to receive the alcohol or drug information, that specially protected information. But all the rest of the regular healthcare data, including allergy information, would continue to flow freely to organization number 3.

Okay, so if we go to the next slide, you will see the second step in this where a clinical workflow event or something happens that triggers this additional information to be sent to healthcare organization number 2, which is the green rectangle. And because this disclosure has been authorized by the patient, the data that requires heightened protection under the existing law gets sent on to the receiving party, along with the obligations and handling restrictions, such as a prohibition on redisclosure without consent. So in this case, the chart that organization number 2 receives, you can see now has little warning triangles next to alcohol and drug information, just to show that that information can't be further redisclosed, again without the consent of the patient in this scenario. And bearing in mind, of course, that medical emergencies and sort of break glass overrides do take precedence and are, in fact, accounted for and baked into the standards that I'll talk about here in just a minute. So I think that lays out the user story.

We can move on to the next slide, and I'm going to talk a little bit about how the standards that have been worked over the last two years and more, to be able to enable this workflow that we've just seen in a pretty seamless way. So we do have a standard, it's the HL7 implementation guide, Data Segmentation for Privacy [Release 1] and this standard completed its normative ballots in January and has been successfully reconciled and it's been approved for publication and has been sent to ANSI for final accreditation and processing. So, we have a fully-fledged, fully completed normative standard. The standard does use document level tagging to convey the confidentiality levels and obligations such as "don't redisclose without consent" or "this document is restricted," and I'll show you some of the well-known vocabularies that are used to actually convey that meaning in a couple of the slides coming up.

So, please consider this standard fully mature and delivered to the community.

Okay, so next slide –

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

Can we interrupt with questions along the way or do you want us to wait?

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

I'll defer to Deven on how you want us to handle that.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

I was going to defer to you, Johnathan. I think – so I think if you think that it's possible that he might cover it in a subsequent slide, then I would ask you to hold off. But if it's actually directly relevant to material that's on this slide, and there's a chance that he's not likely to get to it later, and you can just make a judgment call on that, then go ahead and ask. So David, depending on the category of your question, you can either go or wait.

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

Okay, so I think we'll get into it later, but I'll just ask. Do you think that the normative standard covers your use case?

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

Yes, I do. I really do and I think –

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

So I'll queue up my question, if it's document level tagging how you cover your use case, but I'm sure you'll get to that later. So that's just – consider that a queued up question for you.

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

Perfect, thank you.

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

Because – so, the example showed segregation of some data was allowed to flow, some data was restricted, which it either implies two separate documents or it implied item-specific markup.

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

Yup, got it. I'll try to address that as we move forward through the rest of the slides.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

This is Wes. I just wanted to ask a question about a statement that Johnathan made that wasn't on the slide, but it was part of his commentary. He described it as a mature standard based on having been through a number of HL7 processes. There are a lot of people who don't consider a standard mature until it's been implemented and had revisions based on the implementation. I'm just to understand where you characterize this standard, has it been implemented? Has the implementation gone to completion? Were there lessons learned? Or is it just mature in the sense of having gone through a number of ballots in HL7?

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

Thanks Wes and I'll try to address that a little bit now and a little bit as we go forward through the slides as well –

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Sure.

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

– because I do have some slides that talk to that. But yes, I recognize that it is – there are other standards that have been around longer than this, but it wasn't just HL7 processes that led to the development of this normative standard. The earlier versions of the standard were piloted and tested by the Data Segmentation for Privacy pilots and that input was fed back into both the S&I community and the HL7 community that deliberated over the standard and voted on it. So, it does have real-world experience baked into those processes.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

So, okay, all right. So, I understand your position, thanks.

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

Thank you. All right, so let's drive forward to the next slide. Okay, and I'm going to sort of breakdown the standard a little bit now, so it – the standard contains three volumes; there's a content specification and then there are two transport specifications, one that explains how to use DS4P with Direct and the other with exchange. And I have a couple of slides on these sub-bullets, so, if we move forward. You'll see the next slide talks about the content specification. And so Volume 1 is a CDA R2 and privacy metadata content profile.

And think of this profile as containing the reusable building blocks that other transport specifications that may come down the road, should be able to use in order to implement data segmentation in a different transport or a different architecture. So, this is essentially a transport agnostic content profile and what it effectively does is it associates information such as – information objects such as a document, with security labels, which in turn can be linked to the privacy policies. There's a note here too, that HL7 also built in the ability to specify provenance of clinical data in the structured content of the CDA. So this is a transport agnostic, content profile based on CDA –

If you go to the next slide, it talks about Volumes 2 and 3, which contain the constraints on transport for implementation of data segmentation in a Direct environment and also in an NwHIN exchange environment. And I think it's important to note here, we've been talking a lot about HL7, but IHE have also been actively involved in helping support Data Segmentation for Privacy and are also creating a US realm, ITI technical framework volume that describes, in IHE terms, how Data Segmentation for Privacy is applied in the XDS environment. Okay, next slide.

So, among the – or within the HL7 Data Segmentation for Privacy Standard are a number of different vocabularies and references to other standards, which are also, I think, mature and normative, and have been around in some cases for some time. So, the three that are highlighted in bold and italicized are really reflective of the main building blocks that I alluded to earlier. And so the first of those is the HL7RefrainPolicy. And this is the vocabulary that's used to convey any specific prohibitions or restrictions on the use of that information, such as the prohibition of redisclosure without consent. The second is the HL7PurposeofUse and this contains the purpose – or conveys the purpose of the disclosure of the information. And two good examples of that are, it's treatment or emergency treatment. And then we have the HL7ConfidentialityCodes, and these describe the confidentiality codes associated with the disclosed information, and these are, I think, further described in the now normative Healthcare Classification Standard as well.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Question.

**Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy
Principal – Security Risk Solutions, Inc.**

Yes sir.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Is this a complete list or is this a representative list?

**Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy
Principal – Security Risk Solutions, Inc.**

There is another table on the next slide and I believe that the two tables combined represent the complete list. Could you switch to the next slide please? You'll see here that there are other standards that are referenced and obviously depending on the implementation, there would be other transport standards that would need to come into play. And then if you were implementing Data Segmentation for Privacy in an HIE environment, you would potentially have the need to create a location of a consent directive and retrieve that consent directive and then be able to pass it, and the standard that the DS4P S&I community chose for that was the CDA Consent Directive DSTU. But that's not to say that that is the only way that you could represent the consent. What's important for the DS4P Project is that the sending system that's disclosing the information has the appropriate consent on file before that disclosure can be made and that is consistent with current Part 2 regulations and requirements.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Yes, this is Wes Rishel again. I just wanted to clarify my question. The previous slide listed in essence six different code sets that are used to convey different concepts associated with Data Segmentation for Privacy. And my real question was, how many different values are there in each of those code sets, I mean, one of the issues that has come up in the past about implementing on a large-scale basis of access standards relates to just the understandability of that list of concept codes. If there are three or four, then it's easy, if there are 20, then it's extremely difficult to believe that a lot of institutions will get it the same and if there are 100, then it's impossible. So, I'm just trying to get some order of magnitude of how many values these different code sets have.

**Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy
Principal – Security Risk Solutions, Inc.**

Okay, so if we go back a slide and I have loana on the line as well, who can jump in or I can follow up with you afterwards, Wes, but I think that you'll see, it's a very small number that is constrained for use within the United States. Recognizing that HL7 serves an international community, the US real – this is a US realm specification, and so the – for example, the Confidentiality Codes we have constrained to the use of normal, restricted or very restricted, so that is a very small number of values that can be used for that – to convey that obligation or that restriction.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Okay, thanks.

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

And while we are broken for questions here, these are, as I'm reading the slides – correct, these are vocabularies for document level metadata as opposed to data element level metadata? It's document level –

**Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy
Principal – Security Risk Solutions, Inc.**

Yes, so these are – yes, these are document level, absolutely.

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

So –

**Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy
Principal – Security Risk Solutions, Inc.**

And again, if implementation – I'm sorry, go ahead.

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

Yeah, so I'm just restate what I think that means is something like purpose of use and refrain policy and confidentiality codes would apply to the entire CDA document and by inheritance, to everything within it, even if what's in there is a sodium value or a statement that the person has hypertension.

**Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy
Principal – Security Risk Solutions, Inc.**

So, I'm not a lawyer, I'm not going to attempt to reinterpret the law, but I will convey to you what was said recently to me by a group that's implementing this, and that is that whether or not a particular data element, it could be eye color, right, should be considered sensitive or not is sort of outside of the realm of the standard. And if it comes from a Part 2 facility as part of a Part 2 package, then by nature of that very provenance, it must be protected. If during a subsequent encounter, eye color is rediscovered in a non-Part 2 setting, then eye color is not considered a protected condition, right, or a protective artifact. So

–

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

Right, my concern is how does – when the data gets merged into the actual problem list, which is where providers treat from, they don't treat from these CDA documents, they don't every actually see them, other than the one shot when they may reconcile them into their record. When they're reconciling them into the shared part of the record, problems, medications, allergies and so forth, and the document is flagged as sensitive, but it contains a lot of regular medical information, how does the doctor know what's actually sensitive of the four medicines in the list, which two are sensitive and which two aren't? And how does he rec – keep track of that once it leaves the context of these documents, which is, in fact, what they do, because the CDA is really a message, not a document, in practical terms and real-world implementations. I mean, I know we're going to get into that, but that's – I just want to make sure that along the way I'm not missing something, so I'm – it's document level, but the documents can contain non-protected information, which means we have a question at reconcile time as to how that's sorted out.

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems Corporation

This is –

**Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy
Principal – Security Risk Solutions, Inc.**

I think that's a very – I'm sorry, go ahead.

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems Corporation

Oh, well this is Judy and I'm – I agree with David and a few more questions on that. I'm looking at various things, there's the notes, there's the problem list, there's a diagnosis list, there's a symptoms list, lab test orders, do we hide lab – if we hide medications, and do we also hide lab test orders? And then we have lab test results. The physician, the care team, is it going to be listed everything that gets hidden?

**Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy
Principal – Security Risk Solutions, Inc.**

No, so I don't think that's how this is going to – perhaps I've broken too much into the detailed questions before explaining a little bit more about how the pilots are doing it. But I think the idea is that when you receive a document, at the receiving system, the receiving system alerts the provider that this information is subject to the Part 2 requirements, right, and that alert is based on the fact that this metadata has been attached to the CDA that comes in. Now I don't think the sending system then – if there was to be a redisclosure, I don't think it's a case of going back and finding the original CDA that came in and forwarding it on. I think it's a case of creating a new document that then has the appropriate metadata attached to it, so that the subsequent receiver knows that this is special information or not. So I think that a lot of this functionality will be handled by the EHR systems automatically and will help providers know that information that they want to redisclose is protected.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

I think I'm going to stop the Q&A, only because I feel like now Johnathan, we're really starting to get into the meat of some of this and I think it just makes sense for you to present the material that you have, so that –

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

Okay.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

– we can then have a more fulsome discussion, as opposed to starting it now, before you've finished. So

–

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

Very good, thank you. I do appreciate the questions though, they're great questions, but yeah, let's definitely move on. So, if we jump forward then to the next slide, and the slide after. I think this is where we were. So let's break and talk a little bit about some of the pilot's accomplishments. So for the – next slide please – VA SAMHSA pilot, they successfully demonstrated, in multiple venues, the cap – their capabilities in this regard. They demonstrated an Interoperability Showcase at HIMSS in 2013 and also at the HL7 Plenary Meeting in Baltimore. More recently they demonstrated DS4P capabilities using FHIR resources, and that was at the January, 2014 HL7 meeting, and they used resources from Australia, Canada and USA to demonstrate that capability in real-time.

Next slide please. So NETSMART is one of our commercial pilots and they successfully demonstrated at HIMSS 2013 again, at the Interoperability Showcase. And they have been able to move their Part 2 solution into production with the community services referral network in Tampa Bay, sometimes known as the Tampa Bay 2-1-1 system. And that's helping them manage the restricted data associated with the programs that are covered by 42 CFR Part 2. Next slide please.

So the Jericho Systems/University of Texas/Conemaugh pilot, so they used an external patient consent repository to provide this machine-readable consent information so that it could be processed according to the various privacy policies, as part of any automated release of PHI on the eHealth Exchange. So that's sort of what I was trying to get to earlier, but know that this pilot did use standards based on message formats that are consistent with the current standards and those that I just presented. Next slide please.

So our SATVA pilot, Software and Technology Vendors Association is now part of the Cerner Behavioral Health solution. So Cerner I think acquired Anasazi and Anasazi is part of or was part of that pilot. Cerner did recently report that their Behavioral Health solution will have DS4P using Direct incorporated into full production as soon as April of this year. And at the HIMSS 2014, the Cerner booth demonstrated how marked up CCDs could be sent from the Cerner Behavioral Health Solution over to a Cerner Millennium, their large-scale, general medical solution. And I think it's important to note here that as part of that demonstration, this human-readable 42 CFR Part 2 notice gets displayed at the receiving system's end. Again which meets the – I think the requirements of Part 2 to be able to disclose the notice before fully revealing or when revealing the extra sensitive information that is protected by Part 2. And Cerner also reported that their design teams have been working – have begun work to recognize and be able to process the DS4P marked up data that the Cerner Millennium solution receives from their Behavioral Health solution. And that there are expectations for that functionality to be in production later on this year as well.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

So this is Wes Rishel again. I want to just state the point of view that's guiding my question, which is that demonstrations are never sufficient to prove that a standard is ready to be rolled out across a large industry. They're helpful –

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Wes. I'm only going to interrupt you – Johnathan's finished with his presentation –

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

All right, well just can you ask him to emphasize which of the things he's talking about actually have gone into production and which are demonstrations, that was the point of my statement.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Okay. Johnathan.

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

So the Cerner Behavioral Health solution is having DS4P using Direct going into full production, as we speak, and it will be rolled out in April. And as we saw in the previous slide, if you could go back one slide, please, and I'll just re-emphasize the point here – sorry, one more slide. The NETSMART pilot has their DS4P Part 2 solution implemented, in production, in the Tampa Bay community services referral network.

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

And –

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

Okay, so if we jump forward two more slides, and the next slide please. All right, so I'm going to wrap up here. If you could go to the next slide, so these – again to reiterate and I guess to build on Wes' last question, too, the standards are readily available and they are normative standards. They use widely adopted vocabularies and these vocabularies are not necessarily brand new vocabularies; they've been around in some cases for quite some time. They allow behavioral health systems to better control how this information is handled, and again, focusing on behavioral health systems right now, and to Joy's point about them being typically excluded.

We feel that this – the use of these vocabularies will help convey to non-behavioral health-specific systems, that the information coming in is subject to enhanced security – or is – may require enhanced protection under existing policy and under existing law. And it is our belief that the receiving EHR systems have the technical capability to be able to pass this small amount of metadata, at the document level. And the pilots have demonstrated, and I referred to earlier, we have one significant pilot going into production as we speak and another that's already been in production in Florida. So, I think if we jump forward, it will take us to our question slide, which I'm guessing people are eagerly ready for. So, thank you for the time and the opportunity to present today. I did ask Ioana to be on the line, I think she's listening in but doesn't have an open mic line –

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Oh –

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

– and I also would like to recognize Julie Chua, and thank Julie for her support. Some of you may remember Scott Weinstein, Julie's taken over from Scott in Joy's office for this project.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Thank you very much Johnathan. I suspect people are very eager to sort of follow up on some of the lines of questions involving this – such as the question that David had, but not limited to David's question about what happens with the receiving system when it comes in and Judy's questions. But it sounds like it would be helpful if Ioana had a –

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

Can you hear me?

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Yes, we can, all right, great.

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

Oh, great. Yes, I'm here.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

All right.

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

I was typing furiously.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Okay. Well, since there already are some questions that have been put out there that I think you all have not had a chance to address, because I asked you to get through your presentation first. Do you need them repeated or are you sort of prepared to start addressing some of the concerns that people have begun to raise?

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

Well this is Johnathan, I can begin to, I think, maybe help address some of these concerns. I think that it's important to note that the Data Segmentation for Privacy Initiative didn't try and impose any new policy or any new restriction on already existing workflow, that we've learned from the behavioral health community presents challenges to them. And one of those challenges is their ability to share information with non-behavioral health specialists and yet communicate to the receiving entity that this information is subject to enhanced protection and we've got a way now that is simple in that there are existing standards that are fully balloted.

As we've seen from our pilots and those that are going into production, are fully capable of attaching this additional privacy metadata, so that the receiving system will alert the receiving organization that this information shouldn't be just redisclosed and bundled in with normal healthcare data. If, throughout the course of the encounter, the Part 2 restricted information is rediscovered and so that it is no longer considered Part 2 information, again, I don't think that is any different from how it is today. And we would expect that at the point of reconciliation, that that new information would be entered as opposed to the diagnoses or the clinical decisions that are made purely on the information that's received from the behavioral health system.

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

Johnathan, this is Joy, can I ask you whether you know how, I guess it was – what was it NET – NETSMART, what – do you know what they are doing?

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

The Tampa folks.

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

The Tampa folks, yeah, NETSMART, within that, do you know how their information is handled by the recipient in that case?

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

I think that we can get an answer for that more authoritatively directly from NETSMART, but they have submitted – as a result of their demonstrations and they've presented numerous times to the S&I community, and demonstrated in real-time their live, operational system, which I think there is a video recording of as well. But I think it goes to the point of being a human-readable Part 2 disclosure notice and a restriction on redisclosure without consent notification within the system, so, the obligation from the sending system to have those consents.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

This is Wes. I think that this issue that Joy identified is really – it's certainly at the heart of my concerns and I think others may agree with me, in the following sense. Once information has come in and the notice has been received, there are implications in the law about what the receiving entity has to do with that. One of the arguments for simplicity in this approach is that it is purported to be document-level code, but the – if the information is to be used to the benefit of the patient in the receiving system, it needs to be dealt with at the data item level.

And we are trying to understand whether there is an imputed requirement now, to track the provenance throughout the EHR at the data item level. Or whether there is, if not the purpose of benefitting the patient by having the information shared where it is shared, is lost because it gets lost in a file of reports as opposed to be integrated into the database. And this is why I've been emphasizing wanting to hear the actual operational use, because I think if we can learn how those people who have gone beyond the demo and the pilot stage have dealt with this really big real-world issue, we'll have a lot better understanding of what would be the consequences of trying to roll this out across the country.

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

Wes, this is Ioana, if I may follow up on your question.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Sure.

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

So the first thing I wanted to specify is basically the main reason why we wanted to have a sort of simple annotation be part of the message exchange is that to allow the sender to convey to the receiver the specific obligations related to the data. And you're absolutely correct, the receiver has to process that data and use it for subsequent re-disclosures, that's very important or otherwise this information is exchanged and it does not become useful in any way. So that is definitely one of the conditions of this exchange, that this privacy annotation is conveyed, either at the document level, at the document package level or at a specific entry level, depending on how the sender sends this information. And there have been pilots who have worked at the document level and there have been pilots who have actually annotated each entry, and even they have experimented with FHIR resources and they have annotated specific resources as well.

So in the actual implementation of the standard, people are going to go to the level of detail that makes sense. If something is a 42 CFR Part 2 organization, then the entire document is covered, even if it does not contain necessarily something that would be considered specifically stigmatizing. And that's what Johnathan was explaining earlier that not all the information that's coming from a certain organization may be stigmatizing, but maybe the entire document needs to be managed as a protected piece of information. In other cases maybe specific entries may or may not be protected, and that would be indicated by these privacy annotations.

The contribution of the standards development effort is to ensure that wherever these privacy annotations appear, whether they appear outside a document or document set, they appear within the document or they appear in yet another technology that we have yet to invent, like FHIR resources, they will be represented consistently and they will use the same value set.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Yeah, I'm willing to postulate for this discussion that the standards job has been done very well, it's not – my concern is not whether the standard meets the requirements that we would have on a standard –

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

Right, yeah.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

– my concern is whether implementing the standard will create a burden on the receiving EHRs that is so difficult that this information tends to get buried in a file rather than becoming a part of the active data that is used in caring for the patient.

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

From anecdotal evidence, what I heard from folks is that they do like this idea that they don't have to understand the complexity of the privacy policy and instead, deal with very simple instructions on how to handle the information. So –

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Well I think that's –

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

– yeah, on the anecdotal level –

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

We need to drill down on that as a team, and I think we need other people here in order to do it. But I do think that's an issue that will occupy us as we move forward on this.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

What do you –

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

This is –

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Along those lines, what – I'm going to ask Joy and Johnathan and Ioana and Kathryn, what we think the possibilities would be of having some of – getting some folks from these actual implementations to join us on our next call to talk a bit more about how this has worked. In particular, not – the implementations that do involve the passage from behavioral health provider to a non-behavioral health provider where then the – the regular provider, for lack of a better way to describe it, then has to subsequently sort of deal with the information that may have come to them with a consent. But is now in their hands a mixture of information that is subject to a redisclosure piece, but is probably a mix of data that reveals sensitivity, that the person is a substance abuser, and data that does not. Because I think that would be helpful, if it's possible to do that.

Lawrence Garber, MD – Internist/Medical Director for Informatics – Reliant Medical Group

This is Larry, I think you need to continue with that to think about sort of how this analogizes back to the paper world, where when in the paper world I receive this information in a document, and then I then read that and interpreted it and manually put some of this information into my own system.

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems Corporation

Yes.

Lawrence Garber, MD – Internist/Medical Director for Informatics – Reliant Medical Group

And then what I was allowed to do with it in the paper world versus if it was electronically moved in the exact same way, what the differences are.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Oh yeah.

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

And then what the imply – this is David – what the implications are for downstream functioning if you don't move some of that data into the merged part of the record, but it's actionable data from a safety point of view, etcetera. So, for example in the Cerner demo, as best I understand, we are moving protected documents back and forth between systems with a clear restatement of the constraints on the redeployment, but it's at the document level only. It's not – the data's not being taken out of that document and merged into the target EHR system. Our system doesn't yet have the capability of tracking provenance at the discrete level and I think the rules to do so would be quite complicated, but we can come back to that.

My concern is that if there's a document that has really important medical information in it, and it is on purpose not merged in with the rest of the record, then what happens to safety checks like drug interaction checking? Because those systems don't go against these documents, it would be just impossible to make it work that way, so, what are the consequences to an EHR where you choose to keep it in its segregated document, clearly identified by these new metadata flags, appropriately so. But it's not in the shared part of the record that's being scrutinized for decision support. It gets really tricky and I think the workflow implications for clinicians are where our concerns come from, not that you can't flag documents as being sensitive, I think you've demonstrated that very clearly, and that's a good step forward. But it's the next step that's an inevitable step it seems to me, where we're going to run into the friction.

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems Corporation

This is Judy and I'm totally in support of what David just said. And I think that it's very difficult for people who take – for you to take care of that patient, to figure out why what was done was done if they can't see the reasons that merge with it that say why it was done. And either the doctor has to move everything over into his or her own system, so that people can see that, but that might take a lot of time, or the doctor has to leave it into a place where it can't be redisclosed.

The other question I have is, what – there's a C-CDA document that – what if you go beyond that? What if you're sending more over than the C-CDA document? And that was my earlier question, do you hide the lab test orders? Do you hide the lab test results? Do you hide the referrals? And then, there's other things, too, if you say you hide everything to do with that visit, well what if the patient says, I have a change of insurance, do you hide that? Or do you hide change of address? So I get concerned about that. Another thing I'm concerned about is, you said that you don't hide things if there's a contraindicated drug – well wait, if it's a medical emergency. I'm sorry, you said don't hide things if it's a medical emergency or if – or you can use break the glass. But what if they don't know it's a medical emergency and they're just giving a drug that turns out to be contraindicated? What – even if the electronic health – there's two ways, maybe the electronic health system can't do that, because it's embedded in the C-CDA document, but maybe it can, then what is the system supposed to do? Is the system supposed to do nothing and let you harm the patient? What do you do?

My last question is –

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Hey Judy, maybe – all right, well if this is the last one, go ahead, because I feel like –

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems Corporation

This is the last one –

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

– the response –

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems Corporation

– there's other ways to do this besides this way. Do we have to do it a certain way, this way or can we do it differently. For example, does it have to be opt in, can it be opt out or vice versa? You're saying they have to opt out right now of not disclosing, could instead they opt in to not disclose or, I don't know, I get mixed up which is the out and in, you get the points.

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

Hello, this is Joy, I'd like to –

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

Yes, I'll try to –

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

– may I, may I – first of all, I'd like to go to the specific question that was referred to us by the Interoperability Workgroup, which is, in the context of behavioral health, the regulations have been set on that. They are established, they've been in place for many years and the regulation, and this is not anything that was made up by the Data Segmentation for Policy – for Privacy Project. The regulation requires that a patient consent, in advance, before their health information is shared from certain healthcare providers with others, even for treatment purposes; there are some exceptions such as break the glass. So that's really not a consideration for this group, because that policy is in effect and –

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems Corporation

But there are other ways to do it Joy, instead of this way. For example, –

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

This would not, Judy –

Judy Faulkner, MS – Founder and Chief Executive Officer – EPIC Systems Corporation

– you could have a patient him or herself decide what gets sent and what doesn't get sent.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Well, but Judy, this is in the context of certifying – an EMR voluntary certification standards for a behavioral healthcare provider to be able to move a document out of its facility that – in its entirety because it comes from a Substance Abuse Treatment Program, it's going to be covered by the Part 2. So, there's sort of one piece of it where there has to – there is a need for a technology way to recognize the consent requirements that apply to those providers. And once the provider gets the consent, then they can send the document and the recipient entity has – who the patient has already consented for the document to come to them, can at least use it for their own purposes.

I think some of the questions that David had raised is about well then the subsequent use of the information that's in that document by the general medical care provider who received it. And then I think we have the whole set of issues that I think David and Wes raised very well about how does that all get managed and can we talk to some people that are actually dealing with this today, to understand a little bit better about how they do it. We can't change an opt in authorization that applies to behavioral health providers to an opt out.

M

If –

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

And, because we're discussing it in the context of these providers and their capability to be able to share into the general medical community, and then what happens subsequently to that, that's why the conversation is taking place in that specific context.

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

Could I say –

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

I'd like to respond real quick, if I can to – I'm sorry, go ahead.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

So Johnathan, I'll let you respond and then I think Dixie's next in the queue. And this is not the last bite at this apple, everyone, clearly we have more time to discuss this. But I probably best to actually to be focused on getting questions answered on the standard and the pilots, as much as we can on this call, because we may not necessarily have Johnathan or Ioana on a subsequent call to help us. So go ahead Johnathan and then Dixie.

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

Yeah, thank you. I think just hearing a general theme, a lot of these questions are about what to do with the information when you receive it. What does the EHR system or other system do when it receives the marked up document? How do they handle this information? And what – I think it's important to note that the current sort of situation right now is that information is not flowing. And I'm hearing a desire from the perspective of providers to be able to say that they want that information, they want to be able to access everything. But the situation is that until behavioral health systems can find a way to share this information in such a way that they know it will be protected properly, and according to existing policies; it's just not going to flow. And so there's zero chance of a provider being able to access that information on the receiving end because they're not getting it sent to them.

And so just looking at this sort of from the first steps level, the ability to be able to send information interoperably, between systems. And at the receiving end have the capability to recognize that its subject to certain restrictions is a – I think a huge step beyond where we are today, in terms of the automation of – or the free-flowing of this information. And ultimately the goal is to get the information in the hands of those who need it, not to prevent it from being shared. And this is a means to help get it in the hands of those who need it.

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

If I may add something to that, what I've heard from HIEs is that they are not very interested in getting this information unless they can distinguish protected information with certain obligations from other kinds of information. So, they are welcoming the concept of having more context so they know how to handle this data, so they can build better rules on how to redisclose the data if necessary.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

I think there are two ways to –

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Okay – I think, I'm sorry Wes, I think Dixie was next in the queue.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Oh, I'm sorry. Go ahead Dixie.

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

Thank you Deven and thank you for the presentation, this is a very interesting discussion. What I wanted to add, two things, number one, I think since this NETSMART is a community services network, it's highly likely that that's a behavioral health to behavioral health more of a behavioral health to behavioral health system than a true behavioral health to non-behavioral health. And I – as Joy pointed out, this law has been around for years, and behavioral health systems has been sending information to non-behavioral health clinicians for years and I think what might be really useful to our discussion Deven is to actually have some people talk about how that's done currently. This happens, I talked to Jamie Ferguson about that Kaiser – their behavioral health systems send information to their other system, and it would be interesting to know just what happens now and that could serve as a basis for a discussion on how we adapt it to make it fully automated.

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

So Dixie, this is Johnathan. I think that's a wonderful idea and again, I just want to point out, too that we had a pretty substantial community involved in this project for a number of years. And that community did include providers, so we were able to get their perspective, not just on a one-time shot, but they informed our whole decision-making and consensus process throughout the whole engagement. And so, I've recently been speaking to providers on this very topic and have been asking how they handle this. And the short answer that I've received from most who I've spoken to is that they find it very difficult right now to know what information to share and what not to share because the systems don't help them do that. The systems don't help flag what information is subject to a prohibition on redisclosure and so, what I've been told is that it happens in most part manually, and that really is a very painful, cumbersome, time-consuming process. And the net result is that the information just doesn't get shared the way it should. So, that's what I've heard from the provider community.

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

But repre – this is David, representing vendor community, you've solved the easy problem –

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

Yeah. Yeah, absolutely.

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

– the vocabularies and the tagging, you haven't solved the hard problem –

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

Right.

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

...which is, how to manage the rules governing provenance and sequence and ordering of discovery with respect to redisclosure from automated systems containing a merged record. And until that's put together, I think this is a step in the right direction, but I don't know that there's a whole lot you can do with it other than share these documents and cross your fingers and hope providers can figure out what to do with it.

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

I agree.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

This is Wes. I –

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Go ahead, Wes.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

All right. I think – one point of view, an important point of view to consider is that if we get the ability to certify behavioral health systems to send this information at the document level, we are no worse off than we are now, where they're not sending it. And that may be a platform that makes it easier to make sure the information is useful and perhaps even at some point, create compliance requirements on the EHRs that receive the system. And we could make that decision to go forward, recognizing that the certified capability may end up with the data being kind of quarantined in the receiving system and not available to the deliberations and the automated decision support checking and things like that, until other issues are addressed and that might be a reasonable step forward. I just would like us to be sure, if we take that approach that we understand that we have another can of worms down the beach a little farther that we have to open up.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Yeah.

Lawrence Garber, MD – Internist/Medical Director for Informatics – Reliant Medical Group

This is Larry. I'd like to add to that and sort of actually channel Wes, which is you talked about the concept of bilateral asynchronous cutover. And this is another perfect example where, so okay, so let's say you got the standard, we've got certified behavioral health EHRs and they're able to spit out this document that's got all of the protection metatags tied to it except they have no idea what the capabilities are of the receiving EHR. And it's – there may be some that have now been upgraded to be able to receive these and know what to do with it, but there are others that are going to receive it just like any other document and allow it to be redisclosed. And so – I mean, in the standard, have you thought through how a 2014 certified EHR is going to be able to – what they're going to do when they receive one of these?

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

Yeah, this is Johnathan. So I think, real quick on that, yes, there's a fundamental requirement on the sending system to know that any obligations on the data will be honored by the receiver, and I think that exists today with or without data segmentation, right. So you wouldn't send sensitive information, with or without its tags, unless you knew that it wasn't going to be redisclosed without the proper consent. So you have to trust that the receiving party will comply with the appropriate regulations. But secondly, I think that the human readable notice on the receiving system that is presented as part of the I guess the document XML would present itself back to the receiver. So that there would be an acknowledgment or at least a human readable notice that this information would provide a first sort of safety net for the receiving systems person that's actually reviewing the document to know that this isn't just regular information.

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

If I may add, also on the HIEs I think that's one of the reasons why they are looking for this type of information precisely to keep it out of the hands of unauthorized or maybe less than capable systems. So that would probably be something that on the basis of clear understanding of all the participants to the exchange, an HIE could actually enforce some of these rules. So again, it just goes back to first providing the information, making sure then that it's used appropriately by the receiving system or the receiving HIE and that information does not go into the wrong hands; that's part of authorized disclosure of information.

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

Yeah but wishing it so doesn't make it automated, that's our concern.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Well right, although I have to admit I'm – the way that Wes has proposed the lens through which we should attack this, in terms of sort of good first step, covers the first step in this process, which is getting the documents able to be at least shared by behavioral healthcare providers out of their systems. But then acknowledging that there are challenges with not necessarily the recipient's use of the data internally, but any subsequent redisclosures that they might make because those – subject to some additional digging that we might be able to do with respect to the actual implementers of this, it does sound like there are some remaining challenges on that end. But if, in fact, we are willing to approach this from the standpoint of good first step, needs some additional work to address subsequent challenges, but again, good first step to at least solve the one piece that was missing to date, which is the actual sharing of that information by those providers. But I would –

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

(Indiscernible)

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

– I really am interested in seeing if there are some additional implementation experience, including even how this is typically handled absent the technical capabilities, by providers today who regularly take referrals from behavioral health centers or who regularly treat patients with mixed – where the data is mixed and a combination of some behavioral – information that comes from covered behavioral health programs and information that is not. If there's a – some of those folks, I think it would be helpful.

Lawrence Garber, MD – Internist/Medical Director for Informatics – Reliant Medical Group

So we're going to get –

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

– exogenous input, yeah.

Lawrence Garber, MD – Internist/Medical Director for Informatics – Reliant Medical Group

We're going to get some more information before we declare this a good first step, right?

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Well, yes – but I – that framing of it may be a more helpful way of looking at it, as opposed to necessarily asking it to meet the standards to which we hope ultimately we can go in the future. I mean, that's all I'm suggesting, I'm not saying that we're concluding it, but it just seems like it's an acceptable initial frame for the discussion.

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

So, this is David, and I say this in jest but – I mean only partly in jest, but I think it is a good suggestion but basically it's a better rug to sweep the dirt under.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Okay.

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

So we're moving the dirt downstream and it's probably going to have some good consequences, because there will be more knowledge shared, but it does create a new set of problems in terms of how to automate it, given the way current EHR design works, which is these CDAs are not participating in decision support and alerts and the like. So, perhaps they should, perhaps there are other things we have yet to invent, but standards don't help us with that at this point, unfortunately. Or not.

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

So ex –

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Let me just say that I think exogenous input would be so helpful here, I mean just let's learn a little more and then decide, with our eyes open –

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Right.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

– what is – in some ways it can be progress to move the problem along; it also can be infinite kicking the can down the road but we have a chance to look at that –

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Yeah.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

– after some exogenous input.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Yup.

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

And, and –

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

I have – Deven, it's David, I have one question for Ioana, in case we don't have her on in the future calls, and that's with regard to the standard. It sounded like, Ioana, that you suggested that the standard could be applied at the section or even discrete element level, but I wasn't clear. Is that –

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

Yes. So the CDA implementation guide allows you to annotate a specific entry within a section, if you wish to. If there are – if that particular level of confidentiality is not expressed by the document level, like you say, some things may be a normal confidentiality, but some elements of the document may be restricted or very restricted, so, you can apply those additional annotations at the entry level, if necessary. And some of the pilots have done that, some have not. And that's really where the, I think industry and the real use cases will drive the need and the implementations.

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

I think it's important to note that the standard does not require that and that's a very key take-away from this is that even though the standard would support and does support that sort of specificity that Ioana just described, it is not a mandatory conformance clause within the standard. And if implementers choose not to go to that degree of fidelity, that's perfectly fine and the DS4P approach works just fine either way.

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

Well it –

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

That is important if we understand what they're reaction should be and test for that. So, the problem in general is anything that anyone can send, everyone must be able to process on receipt, so it's much better to give than receive.

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

Well but –

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

The –

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

– it could also – it's a question of who do we expect to do the hard work?

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Right.

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

If the behavioral health expert is unwilling to stratify the restrictedness down to the element level, why on earth should the receiving system be able expected to do that?

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

No, I don't think that's possible, but the other way that I'm concerned about is suppose that a behavioral health does say, well these medications are protected, but these vital signs aren't. Then does that mean that because someone may do it, all receiving systems have to do that or what should they do if they don't? Should they impute the highest restriction up to the whole document level?

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

Yes –

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

Well that's –

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Do we have a way of knowing what highest is in that question?

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

Yeah, so yes they do. So the –

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

(Indiscernible)

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

If I may, Ioana really – if I may real quick, so the standard does account for that and we received a lot of input from not just the pilots, but from EHR vendors and other DS4P participants throughout. And the conclusion was that it's on – the onus is on the sending system to mark the data accordingly, but the principle of the most restrictive, highest watermark applies. So if you apply something at a section level, you must also apply it at the document level and if the receiving system can't process information at the section level, it would default to the document level, which would contain the highest-level watermarks throughout. So, there – that's a –

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

That's –

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

That only helps with half the problem though, because so it imputes upward, but you don't mark the specifics and now the receiving physician has to decide what – which of these 7 medicines is actually the restricted medicine? And is he going to keep all 7 of them out of his medication profile?

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Well again, keep in mind that if the document has been sent from a behavioral health provider, the consent for that provider to use it has already been granted, otherwise the document couldn't have been sent.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Yeah, our whole problem is the ripple effect.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Yeah.

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

It's the redisclosure.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

Right, right.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Yeah.

Wes Rishel – Vice President & Distinguished Analyst – Gartner, Incorporated

If there were no redisclosure, then there wouldn't be much of a problem here.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

You don't have a problem.

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

Yeah, the Dead Sea would not be a problem.

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

Yeah and again, our hope is that the decision on redisclosure could be automated by the EHR on the basis of this additional metadata. And that's really the hope that it's not left up to the individual provider to filter out the data in the case that it needs to be redisclosed.

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

But I think – our concern, Ioana, is that you haven't specified sufficient information to automate the redisclosure and no EHRs are capable of tracking the sequential provenance decisions that would – it would take to do that. So that's a big gap and I suspect if left to their druthers, everyone will do it differently and we'll have a considerable mess.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

So we're – I'm just realizing that we're reaching the end of our scheduled time for the call. We need – I think it actually probably would be helpful, Johnathan and Ioana, if your schedules would permit, at least one of you, to be able to be on standby for additional questions about this particular standard and the pilots in our subsequent discussions. We can go offline to discuss whether that's possible, but we also, in terms of getting some additional folks to speak about how this is handled, both in terms of actual implementation experience with this standard. As well as how people generally deal with this issue today, even if they're not necessarily using this technology standard, is also something that we will aim for on our next call.

We are not, by any measure, done with this discussion, we've really just begun it but I think you all have done an awesome job of teeing up some questions. It's been enormously helpful to at least have the presentation on the pilots and I welcome you all to send emails around subsequent to this call, if there are additional concerns that you want to make sure we tee up for the next call, beyond the ones that we've – that have been obviously surfaced during our discussion. Please do that so that we make sure that we have a really fulsome and complete conversation about this. I fully recognize how sensitive this topic is and how difficult it's been for us in the past. And full transparency and as much knowledge as we can get I think is going to help us come to some conclusions here.

I know Micky had to jump off the call. Does anybody else have anything that they want or need to share subsequent to our next call, before we move to public comment.

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

This is Joy. I would just like to say that it is really important that – and I really appreciate the discussion and the time we're taking to think about this. Because I think all of us recognize that behavioral health is one of the prime issues in this country that's driving healthcare – that's problematic for healthcare and healthcare costs. And clearly these providers are looking to become part of health information exchange. So, this is – this team addresses very difficult subjects and the thoughtfulness is much appreciated.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Okay, let's go ahead and open up for public comment. Thank you. Thank you, Joy.

Public Comment

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

Operator, can you please open the lines?

Caitlin Collins – Project Coordinator, Altarum Institute

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.

Deven McGraw, JD, MPH, LLM – Director – Center for Democracy & Technology

Okay, thank you everyone. Talk to you on our next call.

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

Great, thanks.

Johnathan Coleman, CISSP, CISM – Initiative Coordinator, Data Segmentation for Privacy Principal – Security Risk Solutions, Inc.

Thank you very much.