



**HIT Standards Committee
Data Provenance Task Force
Final Transcript
January 16, 2015**

Presentation

Operator

All lines are bridged.

Kimberly Wilson – Office of the National Coordinator for Health Information Technology

Good afternoon everyone this is Kimberly Wilson with the Office of the National Coordinator. This is meeting of the Health IT Standard's Committee's Data Provenance Task Force. 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 will now take roll. Lisa Gallagher?

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Here.

Kimberly Wilson – Office of the National Coordinator for Health Information Technology

Aaron Seib? Floyd Eisenberg?

Floyd Eisenberg, MD, MPH, FACP – President – iParsimony, LLC

Here.

Kimberly Wilson – Office of the National Coordinator for Health Information Technology

John Moehrke? Rebecca Kush?

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

Here.

Kimberly Wilson – Office of the National Coordinator for Health Information Technology

Mike Davis?

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

Here.

Kimberly Wilson – Office of the National Coordinator for Health Information Technology

And from ONC do we have Julie Chua?

Julie Anne Chua, PMP, CAP, CISSP – Information Security Specialist – Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

I'm here.

Kimberly Wilson – Office of the National Coordinator for Health Information Technology

Mazen Yacoub?

Mazen Yacoub, MBA – Healthcare Management Consultant

Here, thank you.

Kim J. Schofield – Advocacy Chair – Lupus Foundation of America

Jonathan Coleman?

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

I'm here, good afternoon.

Kimberly Wilson – Office of the National Coordinator for Health Information Technology

Is there anyone else from ONC on the line? And with that I'll turn it back over to you Lisa.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Thank you, Kim. I want say welcome to the Task Force members and to members of the public listening in. This is a meeting of the Data Provenance Task Force. For today's agenda we're going to continue our discussion around our evaluation and recommendations for the Data Provenance Initiative of the S&I Framework.

For today we are going to take input from Task Force members per our comments of the last meeting. I hear some noise on the line if everyone could mute please. So, we're going to begin our discussion with a reminder of the specific charge of the Task Force.

We also determined at the last meeting that we would like to have specific and additional time for comment from members of the community and members of the public. So, we do have, on our agenda today, several briefings on related initiatives. We have Robert Dieterle from CMS to give the esMD perspective and we have some panelists, Reed Gelzer, from the HL7 Records Management-Evidentiary Support Workgroup, Gary Dickinson from CentriHealth and Adrian Gropper from Patient Privacy Rights.

Today we will not have anyone from Blue Cross Blue Shield as they couldn't make it to the meeting. So, that one perspective will not be provided today at our meeting.

Do we have Bob Dieterle on the line yet? No we don't Jonathan right? Okay.

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

Correct, I think he should be joining at about 3:15 he just needs to switch over calls.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, so, let's go to slide, let's go to the next slide and see what we have. Panel, discussion, okay, so next slide, next slide, next slide, and one more. Okay, I think Julie there is slide that starts out with the Task Force discussion, it's my slide three but I think the deck has been re-arranged. I'd like to go through the background on our three questions just to remind everybody while we're waiting for Bob.

Julie Anne Chua, PMP, CAP, CISSP – Information Security Specialist – Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Right, so, Kim, I think the presentations were incorporated into the slides that we sent. So, if we can move forward until I let you know when to stop.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay.

Julie Anne Chua, PMP, CAP, CISSP – Information Security Specialist – Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Okay, there.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Let's go through a brief reminder of why we're here and what the scope and the task of this Task Force is. We received a specific question from ONC given the community developed S&I data provenance use case what first step in the area of data provenance standardization would most...be most broadly applicable and immediately useful to the industry. Next slide, please.

In addition, we covered this at the last meeting, next slide, please. We had three supporting questions for us to answer. So, do the three scenarios in the use case and the use case's identified scope, address key data provenance areas or is something missing and that's yes or no and if we feel anything is missing we would provide recommendations there.

The second question, the use case is broad and spans a lot of challenges. Where in the use case should the initiative start in terms of evaluating standards to meet the use case requirements? We have a number of options there. And in some of the discussion that we'll have and input from the public will help inform question number two.

And third, are there any architecture or technology specific issues for the community to consider? And they gave us a couple of examples, areas for us to consider and also wanted to know if there were any other architecture or technology specific challenges that should be considered by the initiative.

Okay, at this point I guess what we can do while we're waiting for Bob is I can open it up to the Task Force members to give us any additional input in the time that we've had since our meeting last week. We asked everyone to think about initial input for these questions and also any scope challenges that you see for our recommendations going forward.

We have I think three Task Force members on today, Rebecca, Floyd and Mike so I'd like to open it up to any of you all if you have any input to help us initially with the questions that are at hand today.

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

So, this is Mike Davis from the VA, so I want to just speak to the standards question a little bit. So, to say first of all the VA has been an active member of the ONCD prov initiative since the beginning and we also work quite actively in HL7 in support of the HL7 DPROV project which is sponsored by CBC working group and co-sponsored by the securing working group which I am a co-chair of.

So, we've also been engaged with ONC with work on what we're calling privacy on FHIR demonstrations and these have from the beginning discussed the need for interoperable provenance metadata in this emerging patient centric health internet of things area.

And so we have recently balloted, last year we balloted, several new standards intended to support the FHIR initiative and these include the healthcare classification system, which was balloted as an international standard and then security labeling services which include a set of services to support the HCS and also some privacy protective services.

So, we have an existing...and I'm a security guy so I'm speaking here principally in the security area with that in mind. So we do see a need for some additional standards in this area and within HL7 what we've been discussing is a couple of things, one is how vocabularies with EHR can merge and coincide so that we're talking the same thing, but more specifically how security can support healthcare in provenance area through data integrity.

So, within the healthcare classification system we have data integrity components, which are not so much the standard security idea of integrity but more of a clinical idea of integrity is to what extent can I trust this information, is it patient provided, is it a lab report from a...is it signed these kinds of things that may influence whether or not that information can be shared with other folks or what the reliability of that information is. So, this has to do with the provenance of it, right? Patient provided information for example.

So, we've been working in that area to develop...to help develop the EHR security area but more specifically in the security area because it is part of the set of standards that have now been put in place to support FHIR. We believe that we have a need for something like a provenance...I won't say it's an entire standard in itself but the existing security standards need an update to at least include a greater degree of discussion in this area.

So, we have things within our existing standards that we would use provenance to help identify let's say the source of a medication, whether that was a sensitive source or otherwise, things of this nature. We're just starting that work and then the HL7, ONC, privacy on FHIR effort will be demonstrating some of this early work at HIMSS this year.

But, I do see that at least within the security area the need for additional standardization work within HL7 and the security and privacy area around providing greater standardization of provenance.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Mike, this is Lisa, and you think that those provenance items they belong in the security standards like do you want to integrate it into that or would you recommend a separate provenance standard or is there one?

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

I don't think we've come to a conclusion on which way to go with that. Just off...my general feeling is that we can incorporate it into our existing standards without, you know...rather than create an entirely new standard, but that discussion...we're meeting next week, I think we'll have discussion within the working group meetings and maybe some other people have opinions here. But it will be a topic of discussion as a new work item for the HL7 security and CBCC working groups to discuss what the best way to go forward is there.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So, I'm hearing the beginnings of perhaps a recommendation that we can think about including from this Task Force. Does that make sense Mike?

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

Yes that's what I was trying to get to as far as, you know, what we see within the scope of our activities within HL7 working with ONC and the development of FHIR and new standards that we definitely see the need for greater understanding of how provenance fits into the total picture.

We have some...I have some limited views, you know, that have to do with the security and privacy areas specifically and some of the stuff...some of the provenance aspects that the EHR group has been working with. So, we've been working with Reed Gelzer and Gary Dickinson and EHR for several cycles already in this area. So...

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So...

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

We want to make sure that we support both security and the clinical side with what we do here but I think there is...the security folks have a definite feeling that provenance is a very important part of the future activities in security and we're definitely going in that direction with some use cases that we're planning to demonstrate at HIMSS.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Great, thank you, Mike. Jonathan, this is Lisa, do you have any input on how the initiative has looked at this aspect?

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

Yes.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

I mean, to me it's an intriguing question.

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

Yeah, no it's a really good question and so the initiative hasn't looked at this particular aspect of it yet with a whole lot of focus because that typically happens during the implementation/harmonization phase of the initiative.

So, what we've done so far in the initiative is to find the use case, right, which we know is fairly broad, probably too broad for us to handle all at once, and as we focus on identifying, you know, which priority areas within the use case we will work on next we will take a look at it from that standards perspective.

So, we'll analyze the standards, the candidate standards that have been identified so far including those which are being developed in HL7 and some of the ones that Mike mentioned are really I think important for us to look at.

In fact, we've had a couple of presentations to the S&I community on some of the FHIR work including the FHIR provenance work which is currently under development at HL7 too. So...

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, so, do we have...I mean on the standards list that you guys have at this point is there anything that we need to add as a recommendations and this is a question for Mike as well as Jonathan?

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

I think we need to add the standard that Rebecca recommended or discussed last time.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Right.

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

...standard and then Mike if there are any other standards that you're working with in the privacy on FHIR project that have, you know, provenance related attributes that we need to look at that we don't currently have on the list we should certainly see if we could add those as well.

Floyd Eisenberg, MD, MPH, FACP – President – iParsimony, LLC

This is Floyd with a comment.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Go ahead, Floyd.

Floyd Eisenberg, MD, MPH, FACP – President – iParsimony, LLC

So, I think having looked over the use cases you sent and the ODM slides that Rebecca sent, Becky, I would agree we would need to add...we should add the ODM standard. In that standard I think it's on slide two of what she had sent, that talks about if there is a change in what's being sent who, why and when did that change occur.

When I look at the...there was a lot of talk last time about...and at the Standards Committee about the use case maybe being overly specified to try to look at every place this piece of data has been but to know it's source, if it's changed, and I think it is an important fact and I think that would be helpful to include the ODM standard for consideration.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Thank you, Floyd. Mike if you are finished, are you...had you completed your input, because we can, you know, continue with any other input that Floyd has, but I just wanted to check back with you? Mike?

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

Sorry, I'm on mute.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay.

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

I'm on mute, sorry.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Oh, that's okay I do that all the time.

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

I missed my brilliant statement there, okay, so now I was trying to just focus in principally on security saying that some of the security standards for the access, control and labeling this kind of thing but probably principally access control needs some additional work to what extent we're not sure but to incorporate, you know, specifically there provenance issues and architectural thoughts.

So, there is lots of provenance work going on in different areas clinically and otherwise depending on, you know, your viewpoint. So, my viewpoint is I think we want, in security and privacy, to be able to really enforce that and we need to then build that into the security infrastructure.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, so in addition to giving suggestions on standards we know about there may be a recommendation to take a look at existing standards such as access control and assess what additional work needs to be done to incorporate provenance. Is that accurate?

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

Correct.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, great. Anything else, Mike?

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

No.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Or any other...

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

Thank you.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, so Floyd, in addition to your input and thank you very much for taking a look at those slides and giving us your perspective, is there any other input from your background work for today?

Floyd Eisenberg, MD, MPH, FACP – President – iParsimony, LLC

Not really and I didn't realize Mike was still going I would have waited, sorry.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

That's okay.

Floyd Eisenberg, MD, MPH, FACP – President – iParsimony, LLC

I guess my major concern is for clinical care, especially if you're trending information and looking at what information over time on a single patient, it's nice to know how much you can trust information so if it's been changed that could make a difference in what you...I mean, your opinion of it and I think the same would apply for research even though we're talking mostly or quality even though we're talking mostly about clinical care in this...directly in this context.

But there are situations where I think it would be very important to know if it's changed for decision support and other uses what's the value of it? Has it changed for the better or the worse, or not at all.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

And Floyd does that...does change include, you know, superseded or amended, or appended to, you know, so we have data that comes in later.

Floyd Eisenberg, MD, MPH, FACP – President – iParsimony, LLC

Well that's what I'm not...when I look at the standards I don't think of it that way. I was thinking more of that particular element. If it's superseded by later data that I would think would be handled in a different way. I was thinking more of if the...well, I guess the question is if it's changed by one provider and then entered into something given to a second provider the origin of the data that is given to the second provider and a change to it is important but if it's superseded the origin might be with the second provider. I guess, I'm not sure how to address that.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Yeah, I think it came up at our last meeting when, I'm trying to remember but the issue is what are the...in terms of trust of the data, you know, what is the temporal aspect of it and I'm not familiar enough with it to have an answer but I thought, you know, maybe we should scope what change means and change means that individual data element as opposed to superseded.

Floyd Eisenberg, MD, MPH, FACP – President – iParsimony, LLC

Well, one thing I was going to suggest is when...and maybe Becky has more information on that, but on the ODM slide where it says "reason for change" is there any structure to that to understand what the meaning of the change is just on that, because we would have to define change pretty clearly.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, thank you, Floyd. Becky, did you want to provide any input at this point?

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

I do, I was going to...I was trying to go back and look at exactly the use cases, but if I go through the supporting questions one at a time I think that the scenarios aren't missing anything if anything they were kind of like we already said, overkill, they were really detailed. And I think the best way to approach this personally is to simplify what we're really trying to get at and that's where I think the FDA's history on trying to track things and look at audit trails and provenance which they've done for ages mostly on paper but now in electronic format is useful.

And if you look at those elements that Floyd was referencing with, you know, who entered the data when, was the data changed, if so, why and when was it changed and how was it changed. And then actually number two isn't so complicated because you can support all of those, you can support A, B, C, D and I would put an E there which is taking data from EHRs and using it for other purposes which Floyd also mentioned like research, quality, public health, outcomes, outbreaks, whatever.

So, we should be able to take EHR data and use it in other ways and track the provenance there as well. And if you look at the commonalities across all of those five use cases tracking those pieces of information around each elements of data can be done the same. And then you still have to over layer the security piece to this, that's content audit trails and you need the security in addition. So, I'm not saying that should be left out.

On item three I'm a little confused by those answers because I think that's probably not how I would answer them but that's interesting and I think there are some others but I'm not really sure how to phrase them yet, they might have something to do with what I just said on number one and two. So, did that make sense?

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Yeah, I think, it does make sense Becky and, you know, with regard to number three, you know, so the Task Force we can interpret the question and provide answers that we think makes sense to us. So, I know you said you're not sure how to formulate them yet and I think that's okay, we can have some of the output, input today and then we can consider what we think we'd like to say with regard to number three.

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

Okay, because if you approach having an audit trail layer or a provenance layer or whatever you want to call on top of the content then it should be able to support C-CDA, FHIR, whatever else should be able to do that. And it's a matter of just layering those pieces of information as you collect each data element.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay that makes sense.

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

I think we really...what I'm trying to say is we don't look at too many specifics on exactly how this should be done and not like someone said, overprescribe it, but take it up a level and say, if you're doing these processes here's the information you need to carry with it to cover provenance.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay.

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

Which also in a way separates the security from the provenance data.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, I mean, that makes sense and I do think we should have further discussion on separation of provenance and pure security data. We understand there is a relationship between them but...

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

Right.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

I'm not sure that aligns yet.

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

So, it's funny because I would approach content and exchange with, well you can exchange using a number of different methods, you know, an ODM is a pure XML exchange but the content for the provenance is just like five or six elements that you want to attach to that data piece so that you can trace it's traceability or even trace what happened to that element.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Right. Sorry, I'm just taking notes here.

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

And...

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Go ahead.

Rosemary Kennedy, BSN, MBA, PhD, FAAN – President & Chief Executive Officer – eCare Informatics

I mean, really where they're going with a lot of this, they call it traceability, they call it trustworthiness, it's really where did that piece of data come from and how much trust can I place in it when it got to where it was going and can I track what happened to it all the way along the line? And, you know, so is it...does it have that data integrity that we're looking for and can we trust that information?

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So, how do we get from those pieces of information to a trust decision?

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

Well...

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So, that the data continues...

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

We really have to track that and in the case of what they do in research, I mean, they go back and they start looking at did the data change and if so why and how was it changed, and that's okay to change things if they're wrong.

I mean, if the FDA sees a field that's changed many times they start questioning whether somebody's manipulating the data or doing something with it that they should look at further. So, it's really a matter of looking back at that information and seeing if there is an excessive number of changes in certain fields. So, you have to take it in the aggregate.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Right.

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

But if you look at one piece of data and say, oh, it went across the way and it came from here and it went there and it wasn't changed then that's great, then you've done your validation and you know that the provenance is there.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, Becky, did you have any other input at this point?

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

No not at this point.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

I mean, we still have the...

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

No, no, no.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, great.

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

That's all I have.

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

Can I comment just on what was just said, because...

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Who is speaking please?

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

So, because...

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Mike?

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

This is Mike.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, great, thanks.

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

Yeah, so the knowledge of where the information came from and its history is important, but...and the changes to the data itself but there are things, you know, in the metadata of the data that you may lose in transport, maybe you lose the signature on the data, you still have the data but now you don't know anything about the reliability of the data because the signature was lost, you got data but you've lost the reliability. So, we need to be able to track and tag the data in different ways...

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Yeah.

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

It's unreliable or uncertain reliability or it is reliable, or it's highly reliable this kind of thing which we need to develop a vocabulary for.

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

That's a good point.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Yeah, excellent point, Mike, thank you. Okay, from the Task Force members any additional comments or discussion at this point before we move to some of the panelists? Okay, Julie do we have Bob at this point or should we move onto the other panelists?

Kimberly Wilson – Office of the National Coordinator for Health Information Technology

We do have Bob.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, great. So, then Kim if we could go to Bob's...the beginning of Bob's slides if they're in here and then we can turn it over to Bob to give us his input. Okay, back, yeah. Julie do you know if we have Bob's slides embedded or are they separate?

Robert Dieterle – esMD Initiative Coordinator – Centers for Medicare & Medicaid Services

This is Bob, they should be separate, I didn't send them until late this morning.

Kimberly Wilson – Office of the National Coordinator for Health Information Technology

We're getting them up.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

All right, oh, great, thank you. Thank you. So, Bob would you like to introduce yourself while we wait for your slides to come up?

Robert Dieterle – esMD Initiative Coordinator – Centers for Medicare & Medicaid Services

Sure thing. My name is Bob Dieterle, I know many of you on the Task Force. I am the contractor for CMS and I am the esMD, the electronic submission of medical documentation, initiative coordinator. I represent the provider compliance group at CMS which is part of the Office of Financial Management and a number of standards organizations including in various aspects or respects HL7, X12 and WEDI.

What we're going to talk about today I believe is the work we're doing with esMD and how it requires and uses provenance both currently and our expectations for the future. Does that give you enough background?

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Yeah, thank you, Bob I appreciate it. And Julie are we close with the slides.

Kimberly Wilson – Office of the National Coordinator for Health Information Technology

I'm sorry, we don't seem to have his slides at the moment.

Julie Anne Chua, PMP, CAP, CISSP – Information Security Specialist – Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Oh, okay, hold on, we had sent it.

Robert Dieterle – esMD Initiative Coordinator – Centers for Medicare & Medicaid Services

Jonathan are you there?

Julie Anne Chua, PMP, CAP, CISSP – Information Security Specialist – Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Yeah, we had sent that.

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

Yeah, I'm here Bob.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Julie, maybe...

Robert Dieterle – esMD Initiative Coordinator – Centers for Medicare & Medicaid Services

You did receive them, correct?

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

Yeah, yeah, we received them and I submitted them. Who needs them and I'll e-mail them right now? Is that Melanie?

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Kim?

Kimberly Wilson – Office of the National Coordinator for Health Information Technology

Send them to Kimberly, kimberly.wilson@HHS, K-I-M-B-E-R-L-Y dot Wilson.

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

Okay, Kim they're on the way.

Kimberly Wilson – Office of the National Coordinator for Health Information Technology

Okay, I'm looking for them now.

Julie Anne Chua, PMP, CAP, CISSP – Information Security Specialist – Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Great, thanks, Jonathan.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, Bob, sorry about that, if there is any...you know, introduction or background that you can start with on the slides we'd appreciate it and then we'll get them up as soon as possible.

Robert Dieterle – esMD Initiative Coordinator – Centers for Medicare & Medicaid Services

That's okay, let me go ahead and set the stage and in fact it will allow us to get through the slides much quicker, we may just jump past it in rhythm. The initiative that we are going to talk about is focused on medical review and submission of medical documentation related to services that are either planned to be provided or have been provided to Medicare beneficiaries. So, that's the scope of what we're working with.

As we will see on a slide that will come up, there has been a significant inappropriate payment rate that congress has asked that CMS focus on and we'll have some numbers for you from audits and reviews that have been done.

So, a large part of what we're trying to do is automate a process that to date has been manual where providers submit information that's required under national coverage determination and local coverage determination rules in CDs and LCDs to establish that a service that is either planned to be provided or has been provided was or is medically necessary and appropriate, which is the basic standard for qualifying for payment for Medicare fee-for-service. Okay, we don't have the slides yet.

So, this initiative, the esMD initiative started, oh, in the mid 2000's and actually wound up with its first production implementation in 2011 and at that point CMS had the ability, esMD had the ability, to receive electronic transactions with documentation. The documentation at that point was PDF so it was either produced directly or stamped. So, we're thinking image documentation with some structure perhaps in a HITSP C62 or basically a CDA wrapper and submission was done over CONNECT or the NwHIN exchange, or its subsequent names.

So, what we're doing at the moment and have been doing for the last three years is expanding the scope of what esMD does which includes the ability to request documentation as well as the ability to receive it electronically. So, we worked on creating the standards to allow providers to register for electronic exchange.

We've created the standards to allow CMS to go and request documentation electronically. So, rather than send out, for example, an additional documentation request letter we can send out an X12 transaction to request documentation using what we expect to be in the future HIPAA standards. Today the request is not a standard at this point in time or not an adopted standard at this point in time.

And then to work on two broad classes of problems, we're calling them electronic determination of coverage, okay, there are the slides. So, let me kind of start the sequence. Go back to the first slide, please, next slide, please.

Okay, so Medicare receives about 5 million claims a day just to give you a feeling for the volume. Based on 2013 audit information, 14 is out but we don't have it in the slides yet, the inappropriate payment rate out of Medicare fee-for-service was roughly 10.1% or 36 billion dollars a year, 27.1 of that was because of inadequate documentation to support that a payment is medically necessary and appropriate, 10.1 billion of it or roughly 1/3 of that inappropriate payment was for services that were not medically necessary and appropriate.

To do the audits, and remember Medicare has a requirement to pay within 30 days of submission of a claim, so in general Medicare pays for services and then goes back and audits and recovers payment where it was inappropriately made. We send out roughly 1.8 million requests for documentation. That is not including the prior authorization programs, the demonstration programs.

The demonstration program for...mobility device for example, if it's fully implemented nationwide, would generate roughly another million documents a year. Next slide, please.

So the goals of the provider compliance groups esMD electronic submission of medical documentation is to prevent inappropriate payment through two broad methods, prior authorization for examples for PMD and prepayment review, in other words, avoid the pay and chase, and start to get to the qualification for payment or the service on the payment.

Try to minimize the provider burden by moving to electronic communication. We are in the process of working on implementation guides for structured information that meet the requirements that Medicare operates under meaning providers have the right to submit whatever documentation they feel is necessary to justify that something is medically necessary and appropriate. We don't set a requirement, we have national coverage determinations most of which allow them to submit whatever they deem is appropriate.

And then to provide digital signatures as a way to establish data integrity and provenance of information and we'll talk about that. So, we promote the standards for all of these electronic transactions, messaging standards, content standards and digital signature standards. Next slide, please.

The process that we described earlier, the ability to request documentation, have it submitted, these are the faces we've gone through. So, before esMD it was all manual, it was a paper letter going out, it was usually a submission back either by fax or by paper. In phase 1, which was brought up in 2011, in September, the responses, as we said were electronic, they were just PDFs, they account for roughly 25-30% of all responses now. And then the next phase of esMD is to send out electronic requests. Next slide, please.

This is...we use CONNECT as a way to communicate with providers or with what we call health information handlers which help to gather information from providers and submit it through CONNECT to CMS.

From CMS, from the Baltimore Data Center and esMD this goes out to the individual contractors that are responsible for the reviews. So, the alphabet soup...the PERMs, the CERTs the Medicare administrative contractors, etcetera. Next slide, please.

This just shows you again another way of looking at registry providers for services sending out request for documentation and giving back medical documentation. This is the flow that we envision on the audit side of it. Now when this becomes prior authorization that flow is different. Next slide, please.

This is a slide that talks about digital signatures. We have done a fair amount of work in this space related to digital signatures including specifications and let's go to the next slide, please, you can review these at your leisure.

We had three different phases of the author of record work which is the digital signature work. The first was focused on signing bundles of documents that are being submitted, okay, so not attesting to their content but attesting to the fact that they're being submitted for a purpose in response to an ADR.

The second or Level 2 was focused on finding individual documents, depending on the nature of the document that could include timing for provenance of authorship and in fact does when it comes to the CDA and the digital signature work we've done with HL7.

And then the third, which is an important part I think for a large part of this conversation, is provenance of information, nonrepudiation signatures at point of origin. Next slide, please.

We've spent a fair amount of time and Workgroup time on looking at identity proofing, digital identity management, digital signatures and the artifacts that can delay digital signatures. We have work that's been done on delegation of rights or the ability of a person to go and delegate the right to sign to someone else. Think of it as the digital version of a Power-of-Attorney. And these author of record concepts related to provenance of information. Next slide, please. Next slide, please.

Okay, so broadly to meet the requirements that CMS has or CMS Medicare fee-for-service the solution has to scale, they're all providers and payers because ultimately all providers and payers or most of them submit requests for payment or prior authorization to Medicare fee-for-service.

To minimize the operational impact required to establish and maintain digital identities and to provide for nonrepudiation without resorting to audit logs or validation of system configuration. One of the issues that we've had with electronic signatures is unless you audit the system, audit the implementation and periodically audit the information including the laws associated with it you cannot provide nonrepudiation behind electronic signature. That's one of the things we're trying to address with digital signatures and we're talking about some of the digital signature standards here that have been incorporated in the work that we've done, Federal Bridge Certificate maybe other authority levels and these are to be consistent with CMS requirements for digital signatures. Next slide, please.

These couple of slides talk about the digital signature and delegation of rights, DSTU implementation guide that was balloted at HL7 and was published. Next slide, please. Next slide, please.

This slide provides a bit of background so the intent is to define a method to embed digital signatures in CDA documents and provides an optional method for specifying delegation of rights and we'll go through this slide in detail, next slide, please, because most of it's summarized on the next slide. Next slide, please.

Okay, so the purpose to provide guidance on the use of digital signatures embedded in the CDA document to provide a nonrepudiation signature that attest to the role and signature purpose of each authorized signer of the document and the way we've designed...and we did a lot of this work with the Security Workgroup from HL7, the way we've designed that ability to sign a CDA allows for multiple signers without affecting the data integrity of what they signed.

It allows us to provide for a delegation of rights, so a definer may delegate that right to someone else. It provides the medical/legal attestation for administrative and clinical information such as documenting transfer of care. And it provides for digital signature, co-signatures and counter signatures and that's all in the work that has been completed. Next slide, please.

So, this really is the summary. So, our current approach is to optionally use digital signatures, we do not require that at this point in time, on CDA documents that provide medical documentation supporting that a service is medically necessary and appropriate.

These need to be produced based on Medicare payment policy prior to billing. The digital signature on the document is attestation on the part of the provider as to their role and purpose for signing both of which are embedded within the signature.

And the use of author participation in the header and at the section and entry levels in a CDA allows them to specify which portions of that CDA they are attesting to for the purpose of their signature whether that's author of particular sections or overall to the entire document.

In the future what we're trying to get forward to in working with the provenance efforts at HL7 and the S&I is the ability to provide a nonrepudiation signature on metadata at the time of information creation and/or review, the review is obviously another aspect of the entire documentation process, to attest to the circumstances of authorship who, where, when, why.

One of the big challenges, and it's been mentioned by people on this call already, is to preserve the content and metadata information including the signature during assembly and exchange so that you can convey the provenance of information and ensure data integrity because the minute we lose that we now have a question as to the actual integrity and value, and provenance of the data. Next slide, I believe that's the end.

Caitlin Chastain – Junior Project Manager – Altarum Institute

Yes, that's the last slide we have.

Robert Dieterle – esMD Initiative Coordinator – Centers for Medicare & Medicaid Services

Okay so that's the presentation. Open to any questions.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So, Jonathan, this is Lisa, is it possible for you to comment on how the initiative has considered this work so far?

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

Yeah, I can certainly try. So, you know, Bob has been very active in the initiative and he has provided his input and the perspective of esMD and CMS throughout the development of the use case. So, I think that we need to continue to work with Bob and to leverage and use his expertise as we move forward but some of the areas that I think we're still wrestling with are, you know, in terms of the use case, how we handle data at point of origin where digital signatures aren't in use and how to persist or what the provenance information should be or should look like potentially in those situations where the data is created for example outside of an EHR system.

So, I think we've got more learning to do and we certainly look forward to, you know, continuing to learn from Bob as we move forward.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Thanks, Jonathan. I'd like to open it up to the Task Force members, do you have any questions for Bob, any comments?

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

Maybe, Lisa, I could build on what I said before and ask the Task Force maybe a more focused question in terms of, you know, the use of digital signatures for data provenance obviously is really key where that digital signature is available and where it is supported, but what...you know, I know digital signatures are used for other things as well as provenance.

So, are there alternatives to digital signatures to get confidence in the truth of source for some of these data elements or documents where digital signatures are not available or may not be possible to be applied?

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Any thoughts from Task Force members on that question, I think it's a good one. Has anyone encountered or used any alternative method to digital signature where it's not available?

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

Usually, this is Mike Davis, usually in this area the question is...becomes a legal one and it has to do with being able to prove that the process is in place or such that someone cannot deny having created some document or done something. So, within a closed system, you know, that's somewhat easier to do they're authenticated locally, you can track their actions and audit trails, you can prove that the processes don't, you know, allow modification and stuff like that.

But, you know, in exchanges between systems digital signatures are the gold standard for how to do data origin and authentication type activities, I mean, proof of...because it provides a framework for interoperable proof of identity and activity. There is a trust framework underneath all those things and Bob did mention the federal bridge certificate authority as being a trustworthy framework for placing the digital signatures and I think this is a question that comes up all the time in the federal space, as well as in the healthcare space, is should we use, you know, all sign up to the federal bridge certificate authority or whether options are there that provide similar or equivalent kinds of trust.

So, it's a matter of the level of trust and how you want to achieve it. Maybe Bob can talk about that. We talk about this quite often.

Robert Dieterle – esMD Initiative Coordinator – Centers for Medicare & Medicaid Services

Yeah, we absolutely do. Mike's pointing out a very important point in that the digital signatures accomplish three things, at the highest level they identify the individual through whatever trust framework they're using, in this case we recognize the federal bridge as the standard for identity proofing and issuance of certificates and requirements for management through their cross certified CAs. So, we're establishing identity of individuals and organizations.

The second is the signature process embedded in it, the declaration on the part of the individual organization as to the role they play and the purpose for signing. So, that establishes the why I'm...what role I'm playing and why I'm doing it.

And the data integrity provided by a digital signature ensures that what they have signed has not been altered from the time they signed it.

So, there are three things we're looking for here and while we're doing it now in a CDA, which means it's an attestation on the part of a signing individual or organization, after the creation of the data, because that's about as far as we can go today given the broad range of EHRs and their capabilities, as long as that occurs before, and again we're talking about Medicare fee-for-service, the billing is in, it meets at least the intent of the policies that are in place. The goal is to have that happen at the point where data is created which is a much more difficult role to achieve as we're all recognizing.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, thank you Bob. Any more questions or discussion on this topic.

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

I'll just make a quick comment, this is Becky, that we do...ODM does support digital or electronic signatures and so that's something that we've been paying attention to and there is one other company out there that does something similar to the one that was just mentioned which is called SAFE and they help with those kinds of attestations and digital signatures.

Robert Dieterle – esMD Initiative Coordinator – Centers for Medicare & Medicaid Services

Yeah, this is...let me make one more comment, this is Bob. We tried to pattern the requirements around addenda proofing and digital signatures to insure certificate assurance, etcetera, were things that are already being done in healthcare. There is actually a fairly limited set on that.

You're either on the federal side, in which case we have examples of that through the...etcetera, or you're doing it on the commercial side or both using something like the digital signature process that was created and is in use for controlled substances by the DEA.

So, the vision is that we want to create as much commonality as possible so that when individuals are identity proofed they get identity proofed one time and one time only or organizations, but they get issued credentials that are appropriate to whatever it is they're going to do whether that's prescribe a controlled substance or sign a document or authorize to a system those are all different things that may take different instantiation of a credential but really comes from a common identity proofing.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, thank you very much Bob we appreciate you coming on the call today. I know you had a conflict and were trying to make it work so we truly appreciate that. Any other final comments or questions for Bob? Okay, so let's move to the panel discussion, Julie and Kim I'm not sure who we should call first, I think listed first is Reed Gelzer. Do we have Reed on the phone?

Kimberly Wilson – Office of the National Coordinator for Health Information Technology

Yes.

Reed D. Gelzer, MD, MPH – HL7 Records Management-Evidentiary Support Workgroup

Yes you do.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Hi, Reed, welcome to the Task Force meeting. I'd like to turn it over to you, I see you have some background on yourself and then you have...Julie we have five minutes for each person to give their input is that correct?

Julie Anne Chua, PMP, CAP, CISSP – Information Security Specialist – Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

That's right.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, so Reed let me turn it over to you.

Reed D. Gelzer, MD, MPH – HL7 Records Management-Evidentiary Support Workgroup

Very good, thank you, if you could just go back one slide. I was trained as an internist and practiced for about 12 years before I migrated into public health, community health and found my way into the electronic health record space. Currently I'm the Co-Chair of the HL7 EHR Workgroup and Co-Facilitator of the Records Management and Evidentiary Support Workgroup.

And I also wanted to echo some notes that Mike Davis made that, especially in the last several cycles, there has been a rapid uptake of community of interest in addressing a number of areas including provenance that have been very beneficial and that though they aren't rendered into full standards yet we are hoping that we will be able to share that benefit with this project.

A couple of other things I want to note is one of my work products was a book published in 2008, How to Evaluate Electronic Health Record Systems, and for that my co-author and I did a methodical evaluation of 38 EHR products and essentially compiled into that vulnerabilities assessments for common areas of EHR variations that can be problematic from a documentation quality, data quality point-of-view.

And I give that as background because I want to highlight that a number of the comments we've heard so far make a presumption that data exists in the source system with regard to things like accurate authorship or actual capture when a record or when a record entry has been amended, altered or updated. That is not a presumption that's reasonable to make in this current marketplace and so that is a key point to one of my responses to the questions asked. If you could...next slide, please.

And for simplicity sake I have simply excerpted a presentation I did as part of a panel for a health policy presentation at Villanova Law School. Next slide.

And if John Moehrke were here he would argue with my separation of security functions from audit functions, I'm not sure if Mike will, but this is a slide I use often in audiences that are composed of people not deeply engaged in Health IT to illustrate how EHR systems are often systems of systems and then large enterprises are necessarily systems of systems and individual subsystems have greater vulnerabilities than others.

And a lot of the discussion about information management and responsible records management and record creation progress really are assisted if we recall that some of these vulnerabilities arise in specific subsystems but not in all, essentially anything where there is a rendering of a note of cognitive processing, assessment that is rendered by a human those are common characteristics of areas of vulnerabilities. Next, please. If I could have the next slide, please.

So, this is an example I often use, an acquaintance who presented to an emergency department with a kidney stone, this is a partial copy of his emergency department record, everything within the red boxes is entirely false and never occurred and anyone who has ever had a kidney stone will particularly note that there is a remark that there is no CVA tenderness, the area on the back that if you have a kidney stone if anybody touches you there you're grabbing for the chandeliers.

So, not only are there blocks of information here that are inarguably falsified significant elements of this record are just plain wrong and you can imagine the impact this has on clinicians trust of records which, as we all endeavor to improve quality of healthcare, still comes down to the bedside patient record. So, this is a national vendor of emergency department documentation systems. Next slide, please.

These are some recent publications and areas of interest that speak to the impact of problematic provenance and therefore problematic trustworthiness of information how it's impacting any number of areas.

The 2012 RFP noted there was specifically looking for a contractor to help with the already recognized phenomenon of using Health IT to gain value-based purchasing by gaining quality measures and we also, I think, will benefit from the notion that our struggles in the healthcare industry with digital records are mirrored by other industries, it's not just healthcare that's struggling with defining trustworthiness and trust.

There are a series of articles there that are publically available through the link that outlines the problem in a general sense and my co-authors and I rendered an article you'll see there specifically with regard to digital records reliability and trust.

And at a recent Johns Hopkins Division of Health Sciences Informatics Conference that I and several colleagues organized for both clinicians and legal scholars to compare notes there were two judges present, one state and one federal, and both noted that knowing what they know about EHRs would have concern about entering them, entering records from them as evidence without substantial scrutiny.

So, this is...so the issue of provenance is one that's deeply complex, far reaching across not just healthcare but other industries as well and we can benefit from that notion. Next, please.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Dr. Gelzer we only have a short amount of time left so if you could wrap it up, thank you.

Reed D. Gelzer, MD, MPH – HL7 Records Management-Evidentiary Support Workgroup

Sure, so, the rest of my remarks and the rest of my input the answers to the questions are all summed in this slide, which is it's at the create clinical data and provenance data for the project to proceed it will be an enormous step forward to either clearly include or clearly exclude the origination of the patient care event record entry. And the rest of my remarks and the rational for that are in the slides. And I'll stop there, thank you.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, questions for Dr. Gelzer from Task Force members or Jonathan?

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

No questions for me I just really appreciate the feedback and the input, thanks so much Dr. Gelzer.

Reed D. Gelzer, MD, MPH – HL7 Records Management-Evidentiary Support Workgroup

Yes, you're welcome.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, anyone on the Task Force, any questions for Dr. Gelzer? Okay, thank you very much for providing us with this input and for attending today, we really appreciate your participation. Thanks, Dr. Gelzer.

Reed D. Gelzer, MD, MPH – HL7 Records Management-Evidentiary Support Workgroup

You're very welcome, thanks for the opportunity.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, so I don't know if Gary is on and I believe Adrian Gropper is on, is that right?

Gary L. Dickinson – Director, Healthcare Standards – CentriHealth

Gary is on.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Gary, okay. Do we have slides for Gary? Kim and Julie do we have slides?

Kimberly Wilson – Office of the National Coordinator for Health Information Technology

Yes.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay.

Kimberly Wilson – Office of the National Coordinator for Health Information Technology

They're uploading now.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, perfect. Okay, Gary would you like to introduce yourself and then as soon as you see the slides we can get started. Okay, I see them. So, you can go ahead, thanks.

Gary L. Dickinson – Director, Healthcare Standards – CentriHealth

Okay, yes, this is Gary Dickinson, I'm Director of Healthcare Standards at CentriHealth, thank you for the invitation to review your questions and provide some perspectives. I have been active in the data provenance initiative since its inception and I've also been active in S&I Framework since 2011. Next slide.

I was asked to put together a brief bio so there it is. I'm also Co-Chair of the EHR Workgroup at HL7. I'm Co-Facilitator of the HL7 EHR Interoperability Workgroup which is a Sub-Workgroup of the EHR Workgroup and I'm a member of the US Technical Advisory Group to ISO TC215 on Health Informatics. Next slide. So, these are the questions, next slide.

So, the first question basically relates to did the initiative miss something impactful? So, I guess I will start this with some basic foundational statements, data provenance is about truth, authenticity and trust assurance. Data provenance represents and embodies the source of truth at the point of data record origination.

Data provenance if properly captured retained, managed and conveyed from the point of origination forward ensures trust to all downstream users and for all purposes to which health information may be applied. Next slide, please.

Okay, so back to the question, we believe in looking at the data provenance initiative that some or many of the fundamental basics are missing. We look at this from the perspective of the data record lifespan and the life cycle events which occur during the course of that lifespan. We look at it from the perspective of the identification of discrete data provenance events. We talked a lot about the point of origination but we also believe that includes subsequent events which may occur to that same data, verification of data content, amendment, attestation, translation to and from exchange objects, and other events which may change or alter the content or in fact may transform the content for various other purposes in that sense.

We also believe that missing is the basic end-to-end showing the point of origination to the ultimate point of access and use. We don't believe that this was consistently represented in the initiative nor in the use cases that are the result of the initiative effort.

We don't believe that there is, again from the stand-point of basics, that there is obvious binding of data in provenance as indivisible, immutable pairs, obviously again starting at the point of origination and preserved and managed from thereon. We think that also there is missing, although it is mentioned a couple of times, the basic end-to-end chain of trust that is described here. Next slide, please.

We were challenged by the fact that the data provenance leadership basically focused, demanded focus on point of exchange as the primary thing. We've really struggled with that throughout the initiative and I think to some degree still struggle with that as we've gone into the harmonization phase.

We focused, for some reason, on assemblers and composers as actors and as the primary focus of use case, user stories and scenarios. We believe assemblers and composers maybe important to actors in the exchange of information and in some scenarios but that we really should be focused on the basics of data provenance not on those particular actors in this context.

We believe also that the development of the CDA R2 data provenance implementation guide was a distraction and particularly since it was done ahead of and was not based on the data provenance community use case requirements. Next slide, please.

So, the question back is, where to start. Again, this is a question that we believe has a very obvious answer and the obvious answer that we've discussed on this call a number of times, again the leadership and systems on point of exchange is a starting point. It took six weeks before the community was able to prevail in the case of data provenance initiative to ensure that the charter, the data provenance charter was explicit, that the place to start is actually the point of data origination.

The charter was ultimately approved by consensus but it was not apparent that this satisfied the leadership of the initiatives as they continued to demand focus on the point of exchange. And I think you can see that clearly when you look at the use case requirements document in terms of the way the user stories, activity, diagrams, scenarios and base flows are presented. Next slide.

So, back to where to start. Start at the first data provenance event, the point of origination binding data and provenance into an indivisible and immutable pair. There may be then a next data provenance event which may be the point of verification, amendment, attestation, translation to or from an exchange artifact and again binds the data provenance pair together. Each of those events and each of those data provenance pairs represent the anchor for a chain of trust.

Obviously we want to ensure that those data provenance pairs are retained in the source system, are exchanged when the information is exchanged and are ultimately retained by the receiving system and made available to whoever may then use that information, may view that information or use it for purposes, particularly for primary purposes of clinical care and interventions. Next slide.

So, back to the specific issues related to software or related to architecture. We believe the software architecture must be designed to manage data records, data and records throughout their lifespan and at each lifecycle event that occurs during that lifespan.

We want to again ensure that the architecture is designed to capture and manage the data provenance pairs from each data provenance event and to share those pairs at outbound exchange to capture those pairs at inbound exchange and to provide access to that data provenance information to end users that is the only way by which they can stand the source or the source context and therefore trust what they're looking at. Next slide, please.

Kimberly Wilson – Office of the National Coordinator for Health Information Technology

Sorry, Gary, we'll need to have you start wrapping up, thank you.

Gary L. Dickinson – Director, Healthcare Standards – CentriHealth

Okay, I'm almost there. So, again software architecture must be based on standards which are oriented to manage the lifespan, lifecycle and data provenance. We believe that there are certainly standards in place for that purpose that can be identified and recognized. Next slide, please.

So, why is there so little uptake? We believe that it's based on the continued focus on the backend for so called interoperable exchange rather than at the frontend where the data originates to ensure data record integrity and measurable quality, the authenticity, source authentication, accuracy, consistency, completeness, non-alteration and data provenance. Thank you.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Thank you, Gary and thanks for participating today. Does anyone have any questions for Gary or any comments on his input?

Floyd Eisenberg, MD, MPH, FACP – President – iParsimony, LLC

Hi, this is Floyd, Floyd Eisenberg with a comment or question actually.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Go ahead Floyd.

Floyd Eisenberg, MD, MPH, FACP – President – iParsimony, LLC

Gary, this has been very helpful. I understand the concern about the origin of data. Has the group you're working with considered a taxonomy for how the different types of origins should be defined?

Gary L. Dickinson – Director, Healthcare Standards – CentriHealth

Well, that's certainly one of the issues Floyd that as it turns out much of the work we're doing of course is in the context, as I'm Co-Chair of the HL7 EHR Workgroup, is in the context of how EHR systems acquire information either directly through user input or from sources such as medical devices or external interface or, you know, interfaces so our focus has been there and also on PHR systems, but we believe that many of these are broadly applicable to many other types of systems. But in terms of a national taxonomy that breaks those out we really haven't done that but I would be interested in your ideas in that direction.

Floyd Eisenberg, MD, MPH, FACP – President – iParsimony, LLC

And the reason I ask is because the origin could be a person which persons have different roles, it could be a device or was it expected to be perhaps the EHR system in which it was entered. I wasn't sure if that had...if you considered that level of what you meant by origin system.

Gary L. Dickinson – Director, Healthcare Standards – CentriHealth

Yes, so we've done a fair amount of work in that area but not a formal taxonomy as you had asked.

Floyd Eisenberg, MD, MPH, FACP – President – iParsimony, LLC

Okay, thank you.

Gary L. Dickinson – Director, Healthcare Standards – CentriHealth

Sure.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So, following up on Floyd's question, would you work at the level of, you know, which person entered the data or that it's, you know, EHR data as origin?

Gary L. Dickinson – Director, Healthcare Standards – CentriHealth

Well, that origin data would be part of the provenance data that you bind to that data item or dataset which would include of course the who, what, when and where type information to fully document the provenance but you could also include signature, you could also include things like identifiers if there is data being captured from external sources or external devices maybe there are identifiers that go along with the transaction, identifiers or other things that allow you to track its origin from that stand-point.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, thank you. Any other questions for Gary?

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

This is Mike Davis, I do have a question, quick question for Gary. Gary, I know you're very knowledgeable in all aspects of security and as a reference point, just talk about audit, you know, audit is useless unless it's turned on, but as you know a lot of systems the amount of data that you get is so voluminous that people turn it off, right?

And so with respect to your end-to-end thing and keeping, you know, the data provenance information at every data provenance event would this not also present a similar problem of retaining voluminous amounts of information that may or may not be useful?

Gary L. Dickinson – Director, Healthcare Standards – CentriHealth

Well, I guess it's a question of what is useful from the stand-point of ensuring authenticity of the ultimate user of the data and so, you know, how much of that should be retained and made available, how much of that should be shared as information goes from one system to another. I think, you know, my bias is to capture as much of that as you can recognizing that it uses a lot of storage but maybe you don't retain it forever on the source system or maybe you archive it after a certain period of time from the source system so that it doesn't remain clutter from that stand-point.

But, again, I think the real question is, what does the end user expect and how, you know, how do you ensure or how do you promote their trust in what they're looking at, what kind of information do they need to know and to be able to see, in other words the original source data was this but, oops when we mapped it to the exchange artifact, the C-CDA for example, and we mapped it to the C-CDA we transformed it when we received it on the other side of the interface, we transformed it again from that C-CDA artifact for internal representation and then the user looks at it, how much of that...how much are they actually able to see of that trace back to the source through the transformations and to what they're now looking at. Are they looking at source data or looking at transformed data, how much of that detail is...and the traceability detail is available to them.

So, I think, these are questions that we still need to work through given that we do have, you know, some of the challenges as you mentioned in terms of the volume of detail that we have to carry along to preserve all of it.

Reed D. Gelzer, MD, MPH – HL7 Records Management-Evidentiary Support Workgroup

This is Reed, may I comment on that?

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Yes, Reed, please do.

Reed D. Gelzer, MD, MPH – HL7 Records Management-Evidentiary Support Workgroup

What you illustrate Mike is one of the technology factors which impinges on this discussion and that is that more recently developed, more modern systems are not as challenged by the metadata capture and managed workload as legacy systems and it's kind of an artifact of the slowness of development of Health IT in the US that systems persist where the only way to get it to speed up is by disabling audit functions. So, that's one factor.

The other part is in the current environment in the survey which I partially updated in 2009 if you established a minimum metadata set that simply was authorship, amendment and a security audit, and particularly security preference functions even a minimal metadata set that meets some basic consensus requirements would be a huge step forward. We don't need to hit it out of the park on the first go.

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

Thank you, Reed, that's good, it makes me think that then, based on your comment, that we have provenance but not all provenance is equal. The data origin event might be very important, the fact that it passed through a certain relay point at some point or not may be irrelevant to clinical use. So, there is sort of like maybe some kind of hierarchy of provenance that we would be more concerned about, you know, capturing than others that would be based on some policy type mechanism.

Reed D. Gelzer, MD, MPH – HL7 Records Management-Evidentiary Support Workgroup

Exactly and some of this actually could be iterative. There is a metadata set that's recognized universally and then for specific uses or if there is a deeper inquiry required then there is no reason to apply in that circumstance a more deep dive, if you will, might not be...a lot of the exchange environments where there is a high-level of trust required and would actually benefit patient care is a much smaller segment of data exchange than most folks may realize.

Working in an emergency department for a number of years I can say that the amount of data that is both time sensitive and highly valuable is really fairly small but it is much better to receive it with a high degree of trust than it is to receive it with minimal trust and huge volumes.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, thank you Dr. Gelzer and thank you to Gary I appreciate your input. I think we should at this point move onto the next panelist, Adrian Gropper. Adrian are you there?

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

Yes, I am.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Hi, how are you? Welcome. Do we have slides for you?

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

No, I'm going to read and I sent in a statement.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, first can you introduce yourself and give a little background and then proceed with your statement, thank you.

Adrian Gropper, MD – Chief Technology Officer – Patient Privacy Rights

Sure, I'm Adrian Gropper, I'm Chief Technology Officer of Patient Privacy Rights and I'm involved in all sorts of interoperability related work including an ONC VA pilot on FHIR that we're doing with Mike Davis and the Health Data Consortium Policy Committee IDESG which is an NSTIC cybersecurity initiative that's also focused on identity, management and the OpenID Foundation HEART Initiative which is a centralized authorization mechanism focused on the resource owner, the patient and the FHIR standards.

So, I'm going to talk about a patient centered perspective on data provenance and I thank you for this opportunity. Good provenance metadata enhances both security and privacy. Your work on provenance can be a real life example of privacy engineering or privacy by design in healthcare.

Security is enhanced when assembled components of a patient's health record are traceable to the responsible party. This also reduces the cost of interoperability by reducing the risk of information intake by a care coordinator or medical home.

Privacy is enhanced when ancillary services such as consumer Apps or HIPAA business associates are presented from abusing personally identifiable information. Good provenance technology is key to assembling a more comprehensive health record from both HIPAA and non-HIPAA data sources.

So, for example Apple Healthkit is one example of privacy engineering provenance and has already seen some adoption by institutions seeking to merge data from external patient controlled services. The key to the Healthkit approach is a separate patient ID for each App or web service that connect to a patient's account. This insulates the various service providers from each other, reduces Apple's risk in assembling highly personal information, allows more transparent control of data sharing by the patient and ultimately makes the combined data more valuable to all.

Good provenance metadata design saves money and improves health. Provenance metadata is only as good as the patient ID. Patient ID is a difficult problem in healthcare and provenance inherits much of that difficulty. Privacy engineering allows us to make progress on provenance even as we continue to work on the broader problem of patient ID.

With respect to question one, did the community miss something more impactful? I would note that provenance depends on three separate identities, the identity of the patient and at least two actors, the actor that ordered and provided a context for a test, and the actor that performed the test and provided a result back to the ordering actor. In all non-trivial cases provenance metadata implies information about the identity of these three actors, the patient, the source and the reporter. Provenance metadata needs to bind these three actors together in a way that's both auditable and private.

With respect to question number two, where in the use case should the initiative start? Privacy engineering suggests that we start with scenario three that includes the assembler/composer where the assembler can be the patient herself. If we can do provenance in that scenario the other scenarios are easy.

Combining safety, security and privacy in scenario three means that the assembler/composer can redact information about the patient but cannot merge information from another patient. All of the result objects in scenario three transactions must be guaranteed to pertain to the same patient even when the patient has had some tests performed under patient controlled identifiers. The assembler/composer can be either an EHR or a PHR.

With respect to question three, are there specific technology issues to consider? Assembling a combination of patient generated data with data from trusted sources and locally generated data requires secure patient ID management by the assembler/composer.

For example, Apple Healthkit in the role of assembler of information from multiple Apps does not share the patient's Apple ID with the App. The patient is identified differently for each App and only the assembler is able to correlate the patient's information across multiple service providers. EHRs and PHRs will both benefit from this approach.

In summary, audits can be designed to reduce the cost and risk of assembling data in an EHR or a PHR. Using cryptographic technology to bind the identity of the patient to the transaction will forestall the need for a general solution to the patient ID problem. Provenance linked to patient consent and accounting for disclosures will save money and improve health. That's it.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Thank you, Dr. Gropper. Any questions or comments from the Task Force members? Okay, well, I'd like to wrap up the panel portion of the discussion today by again thanking every one of our panelists. The information you've provided has been invaluable and given us quite a bit of food for thought. Thank you, all for that.

If we could put the agenda back up, yeah, okay. So, okay, so, I'd like to enter into some final panel discussion and then talk about next steps for generation of our straw recommendations and then approval of final recommendations.

So, looking at our meeting calendar we have one more meeting before I am to present our recommendations to the Standards Committee the last week of this month. So, Julie, remind me of the date of our next meeting next week, please?

Julie Anne Chua, PMP, CAP, CISSP – Information Security Specialist – Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

It is for Friday the 23rd and that is from 9:00 to 10:30 right now.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay. So, our process is going to be that right now we'd like to talk about what we've heard and start framing our recommendations at the very high-level. In between this meeting and the next meeting we will develop, myself and ONC, and MITRE staff, will develop some draft recommendations, I guess we call them straw recommendations which we will send out to you all if we can a significant amount of time before the meeting and we'd like input and comments from you in the meantime on, you know, what you've heard and what...the information that you brought to the Task Force, what do you think we need to put in each of the three recommendation areas and we'll craft that into some straw recommendations.

Our assignment or our take away from this meeting will be to be prepared to review a set of straw recommendations at the meeting on Friday and discuss them and finalize them by the end of the meeting next Friday. We hopefully will leave that meeting with our final recommendations that can be forwarded in time for the meeting materials for the Standards Committee meeting, Julie, which is on which day?

Julie Anne Chua, PMP, CAP, CISSP – Information Security Specialist – Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

The 27th.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So, it's that following Monday.

Julie Anne Chua, PMP, CAP, CISSP – Information Security Specialist – Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Yes.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

And that's really why we need to use the bulk of next week, you know, giving a really good solid set of straw recommendations and hopefully our work on Friday will be fairly straightforward in that we'll try to finalize, wordsmith, whatever we need to do there and vote or affirm those as we go into the meeting on Monday and then, you know, provide any backup information or other information to prepare me to speak to the Standards Committee on Monday.

So, at this point...and that's just an outline of our next steps. This is, you know, a very, very rapid process and we have a lot of information to assimilate. So, again, I want to remind everyone that we're asking you to do some work between meetings and in this case it's going to be particularly important so that by next Friday we have a fairly solid set of recommendations. I will also make an effort to reach out to the two Task Force members who couldn't be here today so that we can get them up to speed and we can get their input in a productive manner.

So, at this point let's open it up for discussion. I think I'd like to structure the discussion in terms of what you heard today, what information each Task Force member brought to the meeting today and where we can start to sort of formulate initial recommendations in the three areas. Does anyone have any initial thoughts?

Okay, well, let's go through each of the supporting questions and if you could put that slide back up Kim I would appreciate it, the one that has the three questions on it. Okay, do the three scenarios in the use case and the scope of the use case address the provenance, the key or most important data provenance areas?

So, I think we've heard some input on that topic and I think what we need to do is to come to consensus as to whether we think that the focus in the three scenarios in the current use case are sufficient or if we'd like to give some advice on how to evolve the use case to address the most key provenance areas.

So, I guess we continue pushing on this discussion. We've heard from several folks that there may be different focus areas that are options for us in terms of the use case. So, is it the point of exchange, is it the point of origin, is there any advice to the initiative as far as how to, you know, evaluate the current use case to try to address that question.

Floyd Eisenberg, MD, MPH, FACP – President – iParsimony, LLC

This is Floyd, I guess I'll take the challenge of being the first to speak up. I think in question two, the first bullet, it seems to be what I'm hearing is the source or the origin source not the EHR itself but how it got there, because I'm not entirely sure if that answer, the bullet of the answer says it all, but it's how it got there, it was manually entered, it was from a device and I think our challenge is going to be how do we identify the device.

There is something called the unique device identifier for implantable devices but it's not quite there for those yet and it's not quite there for say a Glucometer if that's where the glucose is coming from, how it...I'm not sure where you would find it but I think...

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So...

Floyd Eisenberg, MD, MPH, FACP – President – iParsimony, LLC

That's what I've heard so far.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Yes, so we could advise the initiative to perhaps focus some of the standards evaluations on item A, you know, as far as priorities. So, see what's out there as far as standards, see what's out there as far as ways to identify the point of origin and try to factor that into the use case initiative.

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

Lisa, this is Jonathan, can I just ask a quick question just for clarity, please?

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Please?

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

Yeah, so we're talking about point of origin outside of the EHR right as distinct from B which is point of origin inside an EHR for example? So, this would be patient controlled data or patient generated data?

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Right, I mean, that's a question I was asking earlier.

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

Yeah.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

You know what do we mean by point of origin, is it point of origin from the perspective of the EHR or earlier than that?

Floyd Eisenberg, MD, MPH, FACP – President – iParsimony, LLC

I think we need a clear definition, this is Floyd, I think from what I'm hearing, if someone is manually entering it the point of origin is the EHR or PHR. If it's coming from a device maybe a blood pressure monitor or a Glucometer than the point of origin is outside the EHR. So, I think it depends on the data. I'd be interested in other's comments?

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

I think Floyd is right, this is Becky, one of the things that you might want to look at is that FDA has done a lot of work on this and they call it the source not the point of origin but it's the same thing and they had to move from the source being paper to an electronic source so they've just put out a guidance on eSource and these are definitions they've already created.

I mean, you're right Floyd, I mean, any time that the data come from an electronic source originally like a lab or something that's different but otherwise it's whenever the data are first entered and so that's been a thing that has been discussed for years in research.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So, there is some...there is a body of work...

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

Yes, exactly.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Primarily FDA that has evaluated it.

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

FDA just published their eSource guidance which took several years to create based on public input and everything else about a year ago. I can probably find it.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay. I think that's a good reference for us to consider including.

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

Yeah, I just feel like anything that they've already done through the federal government we might as well take advantage of especially if it took a long time to create and not reinvent the wheel here.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So, Jonathan is this work that the initiative has already looked at or was that, you know, something that they could do going forward?

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

No, I think that would be a tremendously useful recommendation to look at that body of work and, you know, this is a dilemma within the initiative, right, is where to start here, because we have, you know, from pick a perspective, it doesn't matter which one, let's say it's an EHR perspective but knowing where the data came from, from a provenance stand-point in terms of patient generated data, a lab, a medical device all of those things have potentially different capabilities and potentially different data provenance attributes. So, you know, how to start is the challenge here. We recognize that it's all important and there are different use cases.

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

That's exactly...

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

Yes?

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

I'm sorry.

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

Go ahead, sorry.

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

Go ahead, Jonathan...

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Go ahead Becky.

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

I didn't mean to interrupt.

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

No, please, I'm done, thank you so much.

Rebecca D. Kush, PhD – Founder, Chief Executive Officer, President & Director – Clinical Data Interchange Standards Consortium (CDISC)

This is really a lot of effort and there has been a big body of work done on it and in fact people have given presentations on where is Waldo, what do you mean by the source, where is the source in this situation and so we were asked by FDA to explore some of this in 2006 I think and we created an eSource data interchange document and that actually informed the guidance that they just put out.

So, this is a big area of interest and it is indeed when they move from everything being on paper to things being electronic and they had to deal with what they called eDiaries which is patient reported outcomes and things like labs and everything else. So, they basically approached it from a set of principles and, you know, requirements as opposed to trying to address each specific case.

Julie Anne Chua, PMP, CAP, CISSP – Information Security Specialist – Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

It's okay...

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Julie?

Julie Anne Chua, PMP, CAP, CISSP – Information Security Specialist – Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Yes?

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, I just wanted to make sure, I think that was your line that was open. Okay, any other thoughts from the Task Force members on formulation of straw recommendations being mindful of the time I'd like to keep in mind that we have to move to public comment in a few minutes, but any thoughts that you all have?

I think Becky and Floyd your input has been really helpful because I think the discussion on where to start and, you know, the focus, you know, being pointed at, you know, item 2A but also the body of work that supports that is pretty significant.

I just wanted to see if there are any other inputs on especially two and three that we can, you know, talk about right now that would help draft the straw recommendations? Okay.

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

This is Mike, I'm somewhat...I haven't, I'm not familiar with some of the recent source work that's been done, but, you know, the question is to me, you know, is almost like when did the universe begin or...

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Right, right.

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

When does life...what's the definition of when life begins, you know, so I don't know that that's a technical problem as much as a policy problem, right?

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Right and Mike this is something we run into on the Standards Committee quite a bit, some of the work that we do, we start talking about technical implementation and we realize that, you know, there are ways to do things and there are alternatives but it really becomes what are the rules of the road that we can all agree to.

I think that if we have a policy consideration that we'd like to bubble up we should identify it. It may not be a recommendation strictly for Jonathan's initiative but it maybe something that, you know, nonetheless we'd like to document. I mean, to me personally with my experiences here I think that's valuable to do.

So, I think you're right, you know, maybe perhaps we can try to formulate some text around, you know, what we think is a policy issue to bubble up, but I agree with you 100%.

Okay, okay it is five minutes till the hour, are there any other final thoughts from the Task Force members? Of course we'll be engaging you via e-mail in the next couple of days but any final thoughts right now?

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

Well, you'll collect the comments from our panels and incorporate them I think that we covered quite a bit there with respect to these two questions.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Right, I think, we got quite a bit of input. I think we have to consider what we formulate as recommendations from that input. So, as I with ONC and the MITRE staff take a look at that early next week we may come to you all and say, okay, here's what we think, you know, we want to recommend, is this right, is this worded correctly, are there any things we're missing.

I think the input has been fantastic but we need to turn that into specific recommendations for the initiative. So, that's where you'll hear back from us. But, I agree with you Mike, thank you. Anyone else?

Okay, Julie and Kim at this point I'd like to open it to public comment. I think we turn that over to the operator?

Public Comment

Kimberly Wilson – Office of the National Coordinator for Health Information Technology

Operator can we please open the lines?

Caitlin Chastain – Junior Project Manager – Altarum Institute

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

Kimberly Wilson – Office of the National Coordinator for Health Information Technology

We have a public comment from Eric Heflin.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Hi, Eric, this is Lisa please go ahead.

Eric Heflin – Chief Technology Officer – HealtheWay, Inc.; Chief Technology Officer – Texas Health Services Authority

Great, thank you, and thanks for the opportunity to provide some comments I thought it was an excellent discussion and very thoughtful discussion today. Obviously, everybody put a lot of thought into their comments that they provided.

I'd like to respectfully suggest that this group consider, one, the use case of including provenance that's preserved across intermediaries and aggregators such for example HIE or similar intermediary that collects data from multiple sources and then potentially aggregates it and sends it back out to other consumers on how provenance will be preserved during that data flow.

Two, consider the issue of multiple sources and destinations such as could be very elegantly handled with something like cryptographic message syntax or CMS also known as secure e-mail which uses that same technology.

Three, there are significant training requirements required of any kind of a similar system requiring end user interaction to both potentially sign as well as verify the authenticity of something that has been signed.

Four, one thing I didn't hear mentioned today was long-term message archiving and retention that we have a use case to retain data for, you know, a number of years while the certificates and the keys may go away the provider of those keys may no longer maintain those and so there has to be some type of way of actually potentially verifying the authenticity and integrity of a message many years after that PKI is no longer actively managing a certificate.

Five, there is actually, from the eHealth Exchange with vendors we've really come across this interoperability issue where we've actually discovered there are multiple types of XML digital signatures and signatures in general and some of which require non-standard processing such as using a pinning kind of a model and I would urge that this group consider constraining the digital signatures to a signal flavor called X.509 which includes the public certificate along with the signature, which allows for standard processing and validation of the signature because essentially it's complete, it contains a certificate in it.

And then finally, please use applicable industry standards some of which were mentioned today. Also wanted to mention a couple, three others, one is IHE's document digital signature standard. Two, is an...standard which standardizes log entries and three, a standard that's actually in flight right now called, actually the name is evolving probably until it's published, but essentially it's a standardized method to query audit logs for functionality or for information contained, so basically it standardizes the interface to access audit logs pulling out that all important information. Thank you, those are my comments and thank you again for the opportunity to provide them.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Thank you, Eric.

Kimberly Wilson – Office of the National Coordinator for Health Information Technology

There are no other...

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, go ahead.

Lauren Wu – Policy Analyst, Office of Policy & Planning – Office of the National Coordinator for Health Information Technology – US Department of Health & Human Services

There are no other public comment at this time, thank you.

Lisa Gallagher, BSEE, CISM, CPHIMS – Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, well thank you. I want to thank the Task Force members as well as our panelists, very good discussion and very valuable input for us. We appreciate everyone's participation. At this time this concludes our meeting today. Thank you, all very much.

Mike Davis, MS – Security Architect – Veterans Health Administration, Department of Veterans Affairs

Thank you.

Public Comment Received During the Meeting

1. I plan to submit the following public comments. Data Provenance. An excellent and a thoughtful discussion. I'd like to respectfully suggest that this consider: 1) intermediaries and aggregators and how data provenance can be preserved in these scenarios; 2) Multiple sources and destinations such as that enabled by CMS (Cryptographic Message Syntax); 3) Training requirements to implement any crypto solutions; and 4) Long term message archiving and retention including validation, which would entail escrow or something similar; 5) There are multiple types of XML digital signatures, some of which require "pinning" another non-standards processing models to validate and associate signatures. I would urge the constraining of XML digital signatures to a single flavor called X509 which includes the public cert with the signature allowing for standard processing and validation of the signature.
2. And finally 6) Please use applicable industry standards such as IHE's Document Digital Signature http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_Supplement_Digital_Signature-2009-08-10.pdf and ATNA http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol2a.pdf and standardized audit log query functionality (which is in progress now).
3. It would seem a reasonable place to start, prior to assuring Provenance Support for PCDs, that the provenance of data clinicians themselves enter at the point of care is supported.
4. Please note that Provenance support does not yet exist for data entered in a given clinical organization's native EHR. Recommend 2b first, with that in mind, as supportive to all other provenance functions. Regarding Mike's comment, regarding where to start, there may be some guidance found in asking what's the main and primary purpose of a patient care record system, and nail that down as a primary objective. Thank you for the opportunity to present. Should there be further questions, my contact information is in the slide set.