



**HIT Standards Committee  
Transport & Security Standards Workgroup  
Final Transcript  
May 15, 2015**

**Presentation**

**Operator**

All lines bridged with the public.

**Michelle Consolazio, MPA – FACA Lead/Policy Analyst – Office of the National Coordinator for Health Information Technology**

Thanks, LaTanya. Good afternoon, everyone. This is Michelle with the Office of the National Coordinator. This is a meeting of the Health IT Standards Committee Transport & Security Standards Workgroup. This is a public call and there will be time for public comment at the end of the call. As a reminder, please state your name before speaking, as this meeting is being transcribed and recorded.

I'll take roll. Dixie Baker?

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

Here.

**Michelle Consolazio, MPA – FACA Lead/Policy Analyst – Office of the National Coordinator for Health Information Technology**

Hi, Dixie. Lisa Gallagher? Aaron Miri? Boban Jose? Brian Freedman?

**Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.**

Here.

**Michelle Consolazio, MPA – FACA Lead/Policy Analyst – Office of the National Coordinator for Health Information Technology**

Hi, Brian. Jason Taule?

**Jason B. Taule, MSB, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems**

Good afternoon, everyone.

**Michelle Consolazio, MPA – FACA Lead/Policy Analyst – Office of the National Coordinator for Health Information Technology**

Hi, Jason. Jeff Brandt? John Hummel?

**John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District**

I'm here.

**Michelle Consolazio, MPA – FACA Lead/Policy Analyst – Office of the National Coordinator for Health Information Technology**

Hi, John. Lee Jones? Peter Kaufman? Scott Rea? Sharon Terry? Steven Lane?

**Steven Lane, MD, MPH, FAAFP – EHR Ambulatory Physician Director – Sutter Health**

Hello?

**Michelle Consolazio, MPA – FACA Lead/Policy Analyst – Office of the National Coordinator for Health Information Technology**

Hi, Steven. And, from ONC, we have quite a few folks on. 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.

**Michelle Consolazio, MPA – FACA Lead/Policy Analyst – Office of the National Coordinator for Health Information Technology**

Hi, Julie. Jeremy Maxwell?

**Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology**

I'm here.

**Michelle Consolazio, MPA – FACA Lead/Policy Analyst – Office of the National Coordinator for Health Information Technology**

Jonathan Coleman?

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

I'm here—hi.

**Michelle Consolazio, MPA – FACA Lead/Policy Analyst – Office of the National Coordinator for Health Information Technology**

Anyone else from ONC? I know there's others that I'm forgetting.

**Rose-Marie Nsahlai**

Rose-Marie Nsahlai.

**Michelle Consolazio, MPA – FACA Lead/Policy Analyst – Office of the National Coordinator for Health Information Technology**

Hi, Rose-Marie.

**Rose-Marie Nsahlai**

Hi, Michelle.

**Michelle Consolazio, MPA – FACA Lead/Policy Analyst – Office of the National Coordinator for Health Information Technology**

Okay, I'll turn it back to you, Dixie.

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

Okay, so the workgroup members are John Hummel, Steven Lane, and who else? Those are the only two I caught.

**Michelle Consolazio, MPA – FACA Lead/Policy Analyst – Office of the National Coordinator for Health Information Technology**

Brian Freedman, Jason Taule, and \_\_\_\_\_.

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

All right. Okay, and who was the other one? Okay, good, great.

Okay, I'd first like to thank you all for joining us today. I especially apologize for having to change the planning for this meeting. I've gotten e-mail from a couple of people who couldn't change the time. Unfortunately, we set it up at the time when I'll be traveling to D.C. next week for the Standards meeting, and secondly, our comments are due Monday, and so having the meeting on Tuesday would be a bit late.

So—so, we erred in our initial planning, but I'm very, very glad that you guys were able to join us today.

Today is the last opportunity for us to review the recommendations responsive to the questions that ONC posed to us regarding the notice of proposed rule making for the 2015 edition of the EHR HIT Standards Certification criteria. Was someone trying to say something? Okay.

Okay, and so we have, we have a couple of—we have several leftover items from, we had action items growing out of the last meeting, we'll go over those, and then we'll briefly go over the, our recommendations on the NPRM. You should have also received a Word document that has our—you know, the full responses. That Word document is the official, the official submittal to the ONC, and that will be what we'll transmit to the ONC as our comments, and today's slides summarize what's in that Word document, so hopefully you've had an opportunity to look at it.

So, our agenda for today is to start by reviewing the action items that were left over from the May 6th meeting. One was that we ask Brian to help us come up with a standard that we might cite for security relevant events to be auditable, and he did a great job, and I think that—I'm pleased with what we were able to come up with.

The second is the, we asked for help on identifying the Data Segmentation for Privacy implementation to date. Then we also had some questions about the electronic submission of medical documentation, or esMD. esMD specification primarily around how the, what appears in the NPRM compares to what the Standards Committee reviewed previously, well, about a year ago. And then finally we'll go over the rest of our comments. Next slide, please.

I wanted to do two things, here. One, I wanted to tell you that there was a meeting of the workgroup chairs with the ONC leadership and the Standards Committee leadership, and the decision was made

that the focus, the primary, top priority for reporting back next week at the HIT Standards Committee meeting are our assessments of the readiness of the specifications that are being proposed as standards. And then the June meeting will be sort of cleaning up on, on any questions that go out of next week's meeting, come out of next week's meeting, and also to discuss any alternatives that workgroups may have come up with.

So, in today's session, we'll start out with a summary of our assessment of the readiness of the various specifications that were recommended, and I wanted to remind you that we do have specific criteria, and they're measurable. I know this is the—this is the graphic that depicts the two matrices that these specifications are judged against. One is the maturity, both of the specification itself and the maturity of the underlying technology and any specifications that that specification depended upon as well, and market adoption also goes into that maturity criteria.

And then the other, the other dimension is adoptability, is the ease of implementing the specification and deploying it across multiple organizations. That addresses how much coordination is really required in an operational environment—the ease of operations and the intellectual property limitations that the specification may have. So we do need to keep—these are the metrics that we're using. The URL for the, for the complete paper that was published by *JAMIA* is there; there's also detailed metrics that are not in the source link there, so if any of you would like to see the detailed metrics, let me know and I'll send them to you. When that article ultimately appears in the physical *JAMIA*, then it will also include a URL to that supplementary material. Next slide, please.

Okay, where—these are the action items from the last meeting on May 6th. Next slide. The three items that I've already mentioned is, we need a standard for security relevant events to be auditable in certified EHR technology. We had questions about how many DS4P—Data Segmentation for Privacy Implementations—there are and how mature they are, whether they are, you know, whether they're pilots or whether they're actual operational implementations that involve coordination among multiple organizations, et cetera. And then finally, the changes to esMD—and it's not just digital signatures, it's also the inherent workflow; the Standards Committee had questions about both. Next slide, please.

We've been, as you recall, I explained this last time, but briefly, there may be some people on the call who haven't heard it—the Security Working Group, both this current working group, Transport & Security Working Group, as well as the Privacy & Security Working Group that preceded it have been asked a number of times by ONC about whether specific actions within a system should be auditable. And when we received this latest question once again regarding this NPRM, we started to look at this more closely and we discovered that the real—the real problem is that the certification criteria for the 2014 edition of the certification criteria don't say that all security relevant events should be auditable. Rather, it refers to ASTM E2147, which only addresses auditable events relating to accesses of protected health information from a database.

And so there was a big gap there, because certified EHR technology should be able to audit—to record audit records of all security relevant events. So, we decided to set out to remedy this and to suggest to ONC how they might close this gap so that it is clearer for both ONC and for the vendors as well as for the consumers of this certified EHR technology exactly what kinds of events in the system are auditable. That's not to say that they necessarily need to be audited, but that the technology be able to record an audit of those events.

So, we, the—our, our—this slide kinda sums it up, is that the current certification criteria and standards don't specify that all security relevant events should be auditable. And so we, our recommendation is that we add a certification criterion that states that certified health information technology should be capable of recording an audit trail of all security relevant events, and that, in addition to ASTM E2147, we recommend adding this NIST Special Publication 800-92—which is audit management guideline, I think is the official name of it—Sections 212 and 213, as the standard for specification of those events that are auditable. Now, ASTM E2147 also names all the data elements that need to be recorded for each auditable event, and that should still stand, but the breadth of the events that need to be auditable would be expanded. Next slide, please.

Here, this is from Section 212 and 213 of the NIST Special Publication 800-92, and these are some of the examples of the type of security relevant events that would need to be auditable. Also, Brian found that the Open Web Application Security Project, or OWASP, has a list of security related events that should be auditable. Now, that—that wouldn't be acceptable to use as a standard, but we did want to bring that to, that reference to the attention of the ONC just to help them put together the certification criterion and standard reference. Next slide, please.

Now, we had—last slide, please. We actually had the wording for this, for the, for the change, but it doesn't appear in this slide. Is it somewhere else, or—? I know it's in your Word document. [Laughter] You'll see in the Word document the specific—the specific wording for, let me see if can find it. Or, Jeremy, can you find it? It's not in this slide, here.

**Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology**

Yeah, let me pull it up real quick.

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

Yeah, I'm sure it's in the—I'm sure it's in the, I'm sure it's in what was distributed. It's in the Word document. Here. \_\_\_\_\_. Well, it's in—I think it's in this section, right here. The—care coordination module. Oh, that's not the right one. All right.

Here—here's the words I'm looking for. What we're recommending and the NIST Publication, 892 is the title, is Guide to Computer Security Log Management. And what we suggest is that the criterion that addresses auditable events, which already exist in the regulation, should be revised to read that auditable events and tamper resistance (1) reports security relevant events. Technology must be able to (a) record the data elements specified in section 7 of ASTM E2147, basically, for all security relevant events performed by the HIT, including the events identified in NIST 892, Sections 212 and 213. And secondly, that events related to access to electronic health information, as specified in ASTM 2147. So, we would add to those. We wouldn't delete what exists, which is the reference to ASTM E2147 for access to health information, but we would add NIST SP800-92 so that it covered all security relevant events.

So, I'm sorry for that interruption there, but I did want you to hear what we're recommending. Is there discussion about this before we go to the next topic? Anybody? And Brian, once again, we really want to thank you for the work you did to help us resolve this issue. It's really, really an important issue, and I think that our recommendation will be appreciated.

**Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.**

You're very welcome, thanks.

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

So, next slide—uh huh, yes. Did somebody say something?

Okay, next slide. The DS4P, these are the DS4P, Data Segmentation for Privacy Implementations. There is—so, Jeremy, can you lead us through the, what are these? Are they all—

**Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology**

Sure, so we invited Kathleen and Jonathan, who have infinite knowledge of the DS4P standards, so Julie, did you—or Kathleen or Jonathan—want to walk us through?

**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**

Sure. Jonathan, are you on? I think you would be the best.

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

Hey, Julie, I'm sorry. Can you hear me okay? I'm on—

**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.

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

- yeah, I'm on audio only at the moment as I'm afraid I don't see the slides, so I don't know, maybe—maybe Kathleen could start and I'll just chime in as needed. Would that be 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**

Sure.

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

Yeah, thank you.

**Kathleen**

Hi, this is Kathleen. I think the first question was some discussion on the implementations that are listed in the deck; 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**

Yes, that's right.

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

Yeah, we're trying to determine mature implementations, but not pilots. Are these pilots, or are these mature implementations?

**Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology**

They are mature implementations. They were demonstrated during the DS4P pilot period, but they are up and running, so the, um, work that was done by the VA-SAMHSA team and others, but have used the model that's now called Consent to Share. It's the SAMHSA Open Source Implementation Specification for doing DS4P with a CEA PS4P implementation guide, and they are using that now. And Ken Salyers at SAMHSA can explain in detail exactly what's going on.

Netsmart, who has also demonstrated their, the way that they had implemented it in Tampa Bay on behavior health and the HIEs down there brought that, brought what they were doing to the pilot, rather than—the pilot was not first and then their implementation.

The most important one, I think, that you might want to think about is Cerner, whose Millennia system is able to do DS4P with the SATVA, which is the behavioral health vendors who have their own approach to implementing the DS4P. They were also in the pilot, and they brought that system and now it interoperates with their Star-EHR product, so we have products in the market that can do this, and I believe that David McCallie has talked about that on some of the calls.

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

Yeah, he has, certainly—he has.

**Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology**

So that's an implementation—that's a major vendor who has these capabilities in place.

Also, Jericho Systems, I believe one of their vice presidents commented at the last call on this topic, and they also have implementations up. Their implementations, interestingly, are in the intelligence community, so they've applied it there and it's being used for segmenting information for their business purpose.

Another place that is not in the health care domain but is a very good place to look for maturity is the aerospace industry. It uses data segmentation to enable competitors in different countries to share information in a way that ensures that only authorized folks can see particular information that's made available in projects.

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

Yeah, but they've been doing that for decades. We're really interested in the uses of the DS4P specifications in health care.

**Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology**

Yeah, well, these three—these three examples, and Jericho, Jericho is actually in the process of implementing it in health care. Another place is, HIPAT has those capabilities in place in Michigan, a sort of statewide HIE, it's a sort of super-HIE, among all the HIEs, and also at Sunnybrook Hospital in Toronto. The extent to which that is actually being utilized, I'm not sure about, but I do know they have that implemented.

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

Okay, so it sounds like we have a reasonable number of beginning implementations, but if you go back to our—back to our criteria, it doesn't sound like it's widely implemented, but it sounds like it's making some good, some good inroads.

**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, I would say these both—I mean, HIPAT's capabilities, and Jericho's, have been in the market for a while, and they, you know, for sure, try to make—they wanted to make sure that the DS4P IT reflected their approach, so it's been out there a while, and so we have DeepField top implementation.

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

Yeah, but neither of those are EHRs.

**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, they are.

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

You know, that's—

**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**

No, they involve EHRs. They are HIEs are managing the DS4P capabilities among EHRs who also do it, so you may want to talk with the principles in those areas to get the details, but they are, live EHR is contributing or exchanging segmentable behavioral health information.

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

Jericho is not an HIE.

**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**

Jericho—I didn't say Jericho, I meant Netsmart and Prince George; sorry.

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

But the rest is—

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

This is Pete, this is Pete—sorry. I'm sorry, Dixie, this is Peter.

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

Mm-hmm.

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

I came on the call late and I'm probably gonna have to leave early, but just so I can get something out of the call—what is DS4P?

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

Data Segmentation for Privacy. It's a specification that was developed through the S&I framework process, and later it moved over to HL7, and the purpose of it really is to enable the electronic exchange of health data that has legal restrictions on it. It used—its first use case was SAMHSA data, behavioral health data, the data that—

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

Mm-hmm, which is a great place to start.

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

Right, right, that you know, if you exchange it, it can't be secondarily distributed, so DS4P is a specification to allow—to allow that.

**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**

And if I got—

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

Sorry to interrupt.

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

No; you're fine.

**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 VA also used, is able to use that, because they have a law that is very similar to SAMHSA's law. It's almost identical, except for that it deals with veteran patients and it has a larger number of covered conditions.

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

Okay.

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

Okay.

**Kathleen**

And Dixie, if I may, the DS4P is really a very simplistic implementation guide. It basically just sets the values that are already in CDAs, so CDAs already have confidentiality codes, and this just says, when you have sensitive information, use restricted rather than normal, which would be for HIPAA. It also merely puts in a text part of the body the specific wording that is required to be shown on any Title 38 or 42 CFR information, and that capability is used for many purposes in CDA already.

So there's no, there's nothing new here, it's just merely trying to ensure that people use the CDA capabilities consistently and for this use case.

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

Yeah, there's nothing; yeah, there's nothing—it is a simplistic specification, but it does entail a difference in workflow, and its integration entailed difference in workflow.

**Kathleen**

Well, yeah, and I kind of looked at that—

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

Thank you, Kathleen.

**Kathleen**

Okay, yes.

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

Did we have some more discussion about this? Are there others who are, I know that David, who's with Cerner—well, I shouldn't speak for him, so I won't. [Laughter] But yes, he has commented on DSP's readiness before. Are there others? John, Steven?

**John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District**

I'm good with it.

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

You're good with it what?

**John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District**

I think that things, the way you have outlined it and your description of where it's in the marketplace readiness I think is good.

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

Well, the way I outlined it is, I don't think it's ready for prime time. [Laughter] I don't think it's ready to become a national standard. I think it's starting to be implemented, but I certainly don't think it's mainstream.

**John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District**

No, what I was reflecting on is, it's not a pilot stage, we've moved—if you take a look at your graph, we're not quite ready for market time, but we're halfway there.

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

Mm-hmm. Yeah, I think that's fair. I think it's further along than where I thought it was, actually, but I don't think there's any way you could say it's mainstream at this point, but, but I'd be, you know— Brian?

**Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.**

Yeah, this is—yeah, I mean, I think Lisa might have been talking about this last time, you know, and I think, yeah, by putting it in, it could become a national standard. I mean, it seems like it's far enough along. Especially with a major vendor like Cerner, having it implemented already, it would seem that—you know, it's not like, I guess my point is that it's not like it's impossible to do or, you know, can't be done. It sounds like there's people using it and major vendors implemented it. So, you know, it seemed that—you know, it should be something that should be moved forward.

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

I'd like to—I'd like to reserve the Cerner comment, because I don't, I don't think that, well, I'd like to reach out to David and see what—David McCallie is from Cerner—and, and get his feedback on this, because I do question, question how, how much that's actually implemented in their, in their technology.

**Steven Lane, MD, MPH, FAAFP – EHR Ambulatory Physician Director – Sutter Health**

I'll also comment—this is Steven Lane, you know, I work with Epic as our EHR vendor, and they're doing a lot of development around this as well, they had a webinar on this just a week ago that I, unfortunately, couldn't attend, but I've got the documentation from it, and they're pretty far along with implementing to this standard.

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

They are implementing it?

**Steven Lane, MD, MPH, FAAFP – EHR Ambulatory Physician Director – Sutter Health**

Yes.

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

So, this is Jonathan. If I may, Dixie, just real quick, I think, you know, in terms of widespread adoption of the DS4P standard itself, I think I would have to concede to you that the spec as it is, is probably not as widespread in its use as, for example, the CDA or the C-CDA. However, because it's based on a number of the existing core standards and capabilities, I think—and looking at the amount of work and effort that has gone into trying to adopt it by real implementations as a result of the work of the pilot, that recommending that it not go forward as a national standard, and even as an optional national standard, would shift the priorities of those who have been pulling this work, you know, just a reminder for everybody, I guess, that the whole point of the data segmentation technology was to enable additional information to flow to authorized providers, not to restrict flow beyond what's already allowed.

So, the use case for allowing those who are in perhaps the most need of having their information shared quickly so that they can receive the kind of treatment they need at the right time is what's gonna be enabled by this standard and its specification. So I mean, if there's more work to be done by pilots or to

see how implementation goes, you know, absolutely, but I think discouraging its use or not recommending its use might be counterproductive to, you know, those patients that really need this.

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

Yeah, really good—very good points, Jonathan. The other point that I would make is that, the way that HIT technology is now being certified, the vendor specifies which criteria they—they, they want to be, want to be evaluated against, although this is—yeah, and DS4P is not in the security list, it's a separate, it's a separate criterion, as I recall from the NPRM. Right? It's not in the securities section; I'm sure it isn't. So, so a—so a vendor could say, "I don't want to be evaluated against that yet."

**Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology**

Yeah, but that—that's correct, Dixie. It is not part of the required, the list of certification criterion that are required to meet the meaningful use incentive program. It is provided as a way for an EHR vendor that has implemented the DS4P standard to be certified that they've implemented it.

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

Well, that—yeah.

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

And—thank you, Jeremy. And if I could, if I also recall, I think that the previous recommendations were for it to be adopted in a tiered approach where the first tier was a very simple capability of being able to receive tag data even as a read-only format, and for that to do optionally which, again, I think the standard supports and allows.

So, you know, if recommending against this, this standard would take away the ability of those who want to certify and are optimally able to do so at that very low level, then it may be counterproductive in terms of the way that those who need behavioral health and other special conditions get their information shared.

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

Yeah, I think that's a—that's a very good point. That's a very, very good point. I think maybe what we should do is, is say what we said. [Laughter] Is that we think it's beyond pilot, but—but it's not ready to be adopted. However, given several—several factors, the, the, the ones that Jonathan mentioned, that we want vendors—you know, it's important, because it does enable behavioral health data to flow, and that, that we want vendors to be able to, to be certified if they've implemented this capability. And—and the fact that it's not part of the security, the security standards, it's a separate, it's a separate criterion, so a vendor could elect to either be certified against it or not, and given those, given those facts, we're not going to, you know, we're going to recommend it stay in there.

Does that make sense?

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

I think that would be tremendous. Thanks, Dixie, yeah.

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

Okay. Thank you, Jonathan, that was very helpful. Okay, and we'll see what, we'll see what, what response we get from the Standards Committee.

Okay. Okay, let's go to the next one—thank you.

Okay, esMD. Electronic—let's see—electronic submission of Medical Documentation. The esMD, when it was presented in the August, 2013 Standards Committee meeting were, there was a lot of discussion, and this, this workgroup, we distributed to you the summary of that discussion as well as, I think we distributed also a link to the, to the transcript as well of the meeting, and the two concerns that the Standards Committee raised were, number one, that the standard for digital signature wasn't well aligned with the already implemented DEA digital signature standard for, for electronic prescription of, of—e-prescribing of medical, of controlled substances.

And so that was one, is the digital signature, and the second, which was probably discussed even more, is that the specification included a lot of workflow that was not, had no currently been implemented, you know, in health care organizations, and would like me to be very disruptive. So, we've asked—at the last meeting, we asked Jeremy to do a compare of \_\_\_\_\_ with the specification that was presented to the, to the Standards Committee. So, Jeremy has asked Bob Dieterle to, to give us that comparison of both, you know, the digital signature standard and the workflow that's inherent in the specification and how it might have been changed since it was presented to the Standards Committee, so—thank you, Bob, for joining us.

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

You're more than welcome, Daisy, and thank you for inviting me to present.

I'm gonna apologize, there's a storm brewing outside, so you may get some background noise from the gods. Let me do the following—a number of things have happened since the last presentation to the HIT Standards of Privacy and Security Committee. So I'm gonna go a little bit through a process here of talking about the background and some of the history and the current status, and also address the issues you've brought up at the same time.

esMD is an initiative that is, as you said, the electronic submission of Medical Documentation, and it is focused on addressing some of the issues that Medicare fee for service needs to deal with, such as managing inappropriate spend which, the last audit was \$45,000,000,000.00 a year. To do this, providers submit documentation, either for prior authorization, pre-payment review, or post-payment audit—those documentations that need to be signed, and we're in the process of moving from basic paper or images of paper, to structured documents; in particular, documents that are consistent with consolidated CDA release 2.

The need to have a signature that provides for nonrepudiation is important. Electronic signatures, unfortunately, require system audits and verification of audit logs to go and achieve that level of attestation. Digital signatures do not, so there's a strong desire to ensure that providers have the ability to digitally sign things so that we don't have to go through the process of system audits and review of audit logs. And, if you remember, the digital signatures establish several things. They establish the authorship of the information—we can talk about how that's done—they establish the time at which the signature occurred, and they provide for a verification of the integrity of the information; meaning that it hasn't been changed from the time it was signed.

The other initiatives within ONC and S&I and, broadly, within meaningful use that have a need for digital signatures are initiatives like VDT, View, Download, and Transmit, where you wish to establish the trust and the integrity of the exchange CDA—the digital signature does that. HIEs that are exchanging CDAs, the ability to go in and ensure that they are unaltered in the event that they are exchanged through an HIE, and to know the origin of the CDA in a way that can't be modified without breaking the signature—the digital signature supplies that.

So, broadly, receivers can, with a digital signature on the CDA ensure that no change has occurred to the document from the time it was signed, and establish the trust for the document based on the trust for the owner of the certificate. So, it provides something that we currently don't have available to us.

As a history, all of the digital signature work that we have done uses the XML DigSig standard, which was introduced by W3C in 2003. That was in response to an EU requirement that was established in 1999 for digital signatures. This standard has been implemented worldwide, and it has been used in the IHE DSG standard, it's the foundation of the FHIR digital signature standard, the Microsoft Word Excel and PowerPoint all support the digital signature standard, and it's the internal standard for digitally signing Adobe .pdfs. So it's very broadly implemented throughout the industry, and used, at least in the context of those areas within health care.

You raised the issue of compatibility with DEA standards. We took a look at that after the 2013 presentation, and this was before we published the Standards with HL7, which actually wound up being published in 2014, the digital signature standard there. The standard uses the same certificates as DEA does. The specification for the cryptographic module to support holding the encrypted private key are exactly the same as are for the DEA—in fact, those specifications, the DEA specifications were copied as part of the NPRM. So, we've made sure that we have identical underpinnings for these digital signatures. The use is different. In the case of the DEA, they're signing a transaction; in the case of esMD, they are signing the actual CDA.

The other thing that's happened since the conversation that we had in 2013 is, the support for digital signatures has now been incorporated into consolidated CDA release 2. And any other CDA guide that utilizes the C-CDA are to Heather, and it's done by utilizing an element in the rim called signature text, which has been incorporated into a legal authenticator and authenticator participant occurrences. So, when someone wishes to digitally sign a CDA, what they do is, they create this artifact that is widely used, the specification for the sake of signing a CDA includes two elements that are not in the general specification, but are accommodated by it. One is the inclusion of a role based on the health care taxonomy code set, which is broadly used in the CDA, and the other is inclusion of a signature purpose, which is an ASTM standard, it's 726295.

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

Okay, we get—you know, really all we needed was, I mean, you have a, you have a captive audience here. We know the value of digital signatures; you don't have to sell us on digital signatures. [Laughter] And all we really wanted to know was whether it was really consistent with what DEA requires, because that's what the Standards Committee brought up. So it sounds like your answer is yes, they're consistent.

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

It is, and to answer your workflow issue, we also went back and addressed the workflow issue, and the way it is specified, the signature on the CDA would occur at the time the CDA is normally signed, okay, because you still have to go in as an authenticator and indicate you're signing it.

And so, as I went through with Jeremy, the only additional work that's required is a two factor authentication to the sign-in module, the cryptographic module, which decrypts the private key and allows the signing to occur. One of the workflow possibilities is when you are going through your day as a provider, anything you need to sign, any CDAs that are created, go into a queue. At the end of the day, you go and you authenticate to the cryptographic module, which takes 10 to 15 seconds, and then just have the software sign each of the outstanding CDAs that you are digitally signing.

So the overhead is really 10 to 15 seconds, and it's only at the time of signing, it's not throughout the workflow.

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

Well, I didn't—when I, when I listened to that conversation, I didn't hear anybody say, “Well, this digital signing”—well, they did say that the infrastructure required for digital signatures would be an imposition on organizations. Which I think it would, you know, I think that still exists, but they were more concerned with its inconsistency with DEA.

So I think you've answered the digital signature questions. What I heard from the Standards Committee was that they were unhappy with the fact that the specification itself embedded a lot of workflow that they would've rather seen functional requirements, like segments of the C-CDA must be digitally signed by the individual who generates it, you know, rather than all the detailed workflow that was in there.

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

Well, remember, what they looked at was the work that was done in S&I, not the work that ultimately wound up at HL7, and—

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

That's what we're asking.

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

- the HL7 work is actually in the NPRM. None of the workflow that you're talking about is actually in the NPRM. None of it. The only thing that's in the NPRM is the specification for the cryptographic module, and the specification for the HL7 standard that tells you what the content is of the W3C digital signature that goes into the already specified C-CDA R2 signature text block. That's it—there's no other workflow specified.

So I think we've addressed all of your issues. We listened carefully, we tried to address them, and make this consistent with implementations that already exist for about 60 percent of providers doing controlled substances.

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

Okay, that's helpful; that's very helpful. So, do you know of anybody who's implemented esMD?

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

We have lots of implementation—you're saying of digital signatures itself? Well, it was not possible—

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

No, no, I'm asking that the specification, the complete specification is what I'm asking.

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

It wasn't possible to implement the specification until C-CDA R2 went to publication.

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

Mm-hmm.

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

So, implementing the signature itself that's going in, there are a number of people that have implemented the signature itself. Putting it into the C-CDA R2, people have done that already. Is it broadly available? No, because we haven't used C-CDA R2 broadly.

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

Mm-hmm.

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

But the mature, I mean—the capability is mature. The impact and workflow is whatever the HIT vendor wishes it to be, and it could be as minimalistic as we said, 10 to 15 seconds, and the standards are all internationally accepted standards and all widely deployed in the U.S.

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

Okay, that's exactly what we needed from you, Bob. Thank you, thank you—that's great, thank you.

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

Let me make one last point—the implementation we did with the Structured Documents workgroup on C-CDA R2 makes, allows for multiple signers at a single document, so you can have two surgeons and an anesthesiologist all sign the same document, and it is both forward and backward compatible, meaning if you don't understand digital signatures and you get a signed one, it will not affect you, and if you get an unsigned one and you expect it, you'll have the ability to deal with it.

So we tried to make this as easy to implement in the industry as possible.

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

Okay. Did you consider just putting up a web service so that people could just come in and submit their documentation and digitally sign it there?

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

That was, the implementations can be either within the workflow or the EHR, or it could be an external web service. We're not trying to specify the implementation, we're just trying to go and say that EHR should have the ability to certify that they can do it, either through an internal service or an external service.

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

Oh, okay, okay.

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

There is no requirement that it be embedded inside of the EHR technology, but rather that it be a capability that is certified for.

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

Okay.

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

Yes, we've tried to listen very carefully, we thought the feedback that we got in 2013 was exceptional, and I think we've tried to answer all your questions.

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

Yeah, I think you've done a great job—thank you. Today, certainly—yes, thank you. We really appreciate you joining us today, and, and responding to the Standards Committee's concerns.

So, let me open up the floor for discussion on this. Are any of you familiar with—John? We probably need you.

**John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District**

I'm sorry, Dixie, could you repeat your question?

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

Yeah, are you familiar with esMD? How would you assess its readiness?

**John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District**

From what I've seen of it and what I've read through, all the documentation, including the C-CDA 2, I think it's pretty ready, I think it's recognizable in terms of other industries and how it's used, and I really like the backwards compatibility that Bob pointed out.

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

This is Peter—are there any downsides to using this? I mean, obviously, we want to do something that's already an established standard, especially if it's being used worldwide and other things, that would make it a great thing. So are there any downsides to this that we should be considering when we're considering using it, or recommending it?

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

Is that a question to me, or—

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

Yeah.

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

Well, you would probably know better than anybody, and I figure you're more than willing to be honest about it, but if anybody else knew anything, then they can come up with it, too, but yeah, it's just—mostly for you.

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

We, we—we wrote it to have zero impact if it is not used, and if it's used, to have zero impact if you can't understand it. The only overhead would be some additional data in the CDA. If you understand what a digital signature is as a receiver, then yes, you have to do some work to evaluate it, but you've already made the choice to receive it and evaluate it so, again, there's no work above and beyond what the receipt of any digital signature requires.

So, I, I—I would term that as minimal downside.

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

So it sounds like, Bob, there really is not wide adoption operationally, because C-CDA, as you pointed out, R2 is relatively new, so there aren't implementations widely available. Do you know of vendors who are implementing it already, or have implemented it already?

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

We're, we're—there are three vendors that are in the process of implementing it, they're smaller ones, and we have spent time as we created the HL7 standard talking with the larger vendors and making sure that it was compatible with the work they were doing for DEA. So, yeah, when you evaluate—for example, when you evaluate a digital signature on an order for a controlled substance, or if you create one, it's the same technology; there's really nothing different there. So the evaluation process is the same. The only thing you have to do differently and, to be very clear, is when you digitally sign something, you compute what's called a hash. That's a mathematical algorithm that goes through the thing you're signing and computes a string, and that string has two characteristics—one, it is mathematically unlikely it could be created from any document other than the one you're signing or any transaction, and the second one is, it's mathematically unlikely that you could recreate the document from the hash.

So, you compute this, and so the way you compute it over a CDA is different than the way you compute it over a transaction. But once you get done with that, the way you sign it and the way you create the artifact and the way you embed it are really all the same.

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

Yeah, the way—the way you do a digital signature, any digital signature, a data object, involves generating a hash, so that's nothing unique.

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

Right, correct, because we had to specify uniquely how to do it on the CDA in a way that allowed multiple signers, and we worked with John Mirke and we worked with the Security workgroup at HL7, and we worked with the Structured Docs to make sure we did it in a way that maintained the integrity of the document while allowing multiple signers to sign.

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

Yeah, yeah—good, good.

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

I think the point of this is, this satisfies a real need we had and the ability to go and guarantee integrity of the document and guarantee who has signed it and, through the offer participation, to allow them to

indicate what part of that they have offered—those things don't really exist in the CDA world today, short of this, and it's also the foundation for what they're doing in FHIR. By introducing this as a certification criteria, we wind up taking the only existing international standard for digital signatures, and specify, specifically, how it should be used so that we don't wind up with multiple ways of trying to find things, find CDAs going forward.

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

But it is, the standard is more than just how do you sign a CDA, it's—

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

It's how you, it's how you—how you compute the hash, how you create the artifact, which is a W3C artifact, how you embed it, and then it's how you analyze it on the other end, but the how you analyze it on the other end is exactly the same as you would analyze any digital signature using a W3C standard. There's nothing unique about it.

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

So you're saying that lets in the—because I remember in the NPRM, there are, there are lots of pages of this for esMD, right? It's multiple pages.

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

Well, we had to specify the cryptographic module because you have to have a place to securely store it, and it's the same cryptographic module description that was used by the DEA.

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

Yeah, I did notice that—yeah, yeah.

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

Okay, and we had to specify the, the, the guide, okay, so we did that, too. So those are the things related to digital signatures in esMD.

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

Now, I'm asking you, the whole esMD specification that's in the NPRM.

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

Okay, well, we [Cross talk].

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

I read the question. It's not just digital signature, there seemed, to me, to be a lot more to it than just, "You shall sign—here's how you're going to sign your CDA."

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

There are two separate pieces to the NPRM esMD work. One is around digital signatures, which we've just discussed and applied. The second is around an implementation guide that sits on top of consolidated CDA release 2 called Clinical Documents for Payers that takes the C-CDA R2 and provides some additional constraints, meaning, specifies that certain sections that are purely optional in C-CDA R2 are constrained to at least be testable in this guide. So it satisfies one of the other problems that we've had traditionally, is that we don't have ways to test optional elements or optional sections in a consolidated CDA that are called May because the conformance process doesn't test optional sections.

This creates them as a shell section so that they can be tested formally in a test tool, but also specifies how to use the null flavors, which are part of all of the CDAs going back to C-CDA R1.1 for regulation and says that if you don't have the information, you can put it what's called no information, an NI, and if you wish to withhold it, you can use the NA, which is not applicable. These are standards that have existed all the way back in CDA, and all we did was specify how you can use them so that providers don't need to collect information just so that we can validate that the section is supported, and they don't need to provide it if they don't wish to provide it under meaningful use. So that's what the other piece of it is, is this CVP1.

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

Okay, okay.

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

And what that does, it allows us to make sure that providers can always exchange, through certified technology, whatever it is they deem is appropriate to exchange, and that was important because we have situations in particular for Medicare fee for service where, if you don't supply enough information to show that something is medically necessary and appropriate, but that you can be—that beneficiaries could be denied services that are prior authorized, providers could be denied payment either as pre-payment review, or have payment requested to be returned through post-payment audit. Not because of anything they did wrong, but because the CDA, as was tested and certified, didn't support the information that was already in the EHR, but hadn't been tested to go into an optional section.

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

Okay, I think we have a—I think we have a good, a really good feel for, for how mature and how—certainly how mature. And I think that, I think based on what you said, clearly you've done a lot of work since you've presented this to the standards committee, and I'm sure that one of the things that we should make clear, Jeremy, in our slide systems is that we should make that very clear, the additional work that's been done since it was presented.

I think, if we go back to our metrics, I don't see any way we could say that this is ready on either of those matrices. I think that, as you've pointed out, the maturity of the underlying technology is pretty good, because they're using existing standards for digital signature that's been around for quite a while. CDA R2 hasn't been around for a long time. The maturity of the specifications certainly can't be judged mature. It's a new specification, and on the adoptability criteria, we have no idea how easy it is to implement, nor do we have any idea how easy it is to use it in operations. We know it's good intellectual property because it's an open standard, but I—but I don't see any way we could possibly step up and say this is, this is mature and widely, and widely implemented and adoptable. You know, I just don't see it there.

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

I think, Daisy, much like we talked about—

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

My name is Dixie, by the way.

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

- I'm sorry, Dixie; I apologize.

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

Oh, no problem; I just wanted to clarify.

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

Yeah, thank you, and I'm sorry.

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

No, there's no need.

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

I think the issue is to make sure that vendors can certify to it. esMD has a need for it very strongly. It looks like the other areas like VDT and HIE have a need for digital signatures, and standards that can be used for implementation of more exhaustive testing of CDAs. I believe it's one of the optional criteria, so this is something that an EHR vendor can elect to do as opposed to is required to do, so we're not forcing [Cross talk]—

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

[Cross talk] this is the only lever that ONC has to encourage piloting of such standards. I personally think it would be much more appropriate to encourage ONC to support piloting of this than it would for us to step up and say, "Oh yes, this is mature and easy to implement"—we have no idea. Is there anybody here who thinks that this is something that is, yes, ready to become a national standard?

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

Well, I'd have to see more about it. I think that it's an early presentation, and I was on a committee in 2013, but you know, as a vendor, I'd like to see how amenable it really is to see some of the spikes on it.

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

Yeah, I think we should, we should really applaud the work that's been done since it's been presented to the Standards Committee, because obviously they listened and they followed up, and that's really—you know, that's really something to be commended. I think we should say that, you know, and mention that it is, that how—how they followed up. And I think that we should strongly encourage ONC to support piloting of this new, of this specification so that it can, so that we can accelerate its maturity and the determination of how implementable it is. But I don't think that we should say it should be a standard at this time.

**Steven Lane, MD, MPH, FAAFP – EHR Ambulatory Physician Director – Sutter Health**

I agree, Dixie—this is Steven Lane.

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

May I ask one question, Dixie?

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

Mm-hmm.

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

If we don't provide it as a certification capability—

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

Yeah, I actually responded to that. There are different levers that ONC has. Certification is one of them, and it's one—it's a very serious decision when you put into law that every vendor has to implement this standard. A standard is a big, that's a serious decision and not one to be taken lightly—to say to the world that we think that this is ready to become law, I think it would be irresponsible.

I think that it is responsible to say, use another lever to say, “We think that ONC should encourage and support”—that means put money and resources and people behind, pushing for its piloting and, and, you know, and its further maturation and further development, but I don't think that we should say it should become law.”

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

So, Dixie, my question was, if it's an optional certification criteria, it is not mandatory for everyone—in fact, there's no requirement that any actually certify to it, but it does become available through the certification process for those that wish to.

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

Right. I don't think it's ready even for that, because it's—that's law. [Laughter] You're putting it in there, and you're saying, “This—this is the specification.” I suspect that as they do pilots, as you do pilots around this, that specification will be further refined. It won't end up—the specification itself will be further refined, it'll be made easier to use, easier to implement, easier on all those metrics they use to determine when it's ready to become a national standard, and I think that it will benefit from having that opportunity. I think you will benefit hugely from having that opportunity.

So I think that's what will be our recommendation. Okay, let's go on to the next slide. Thank you, Bob.

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

You're welcome.

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

Now we're going into our final comments on the NPRM. These are, we should be able to get through these fairly quickly, because they're, we didn't have further questions, but we wanted one last look at what's here. Next slide, please.

The NPRM proposes a new approach to privacy and security certification. It says that HIT modules that are presented for certification will be certified against all of and only those security and privacy criteria that are identified in that chart as relevant to the functionality provided, and using either of two approaches, either to technically demonstrate compliance or through system documentation. Next slide, please.

And you know, I think we said in our written, we did, in our Word document, we did say that we agree with this and we appreciate the change, we think it's a good thing, so we, so we prefaced it with that, because what they're doing is proposing what this working group has proposed before. So we, we do—we do feel they're going in the right direction.

The only recommendations we have are the addition of a couple of criteria to the clinical type, those modules that are being certified against the clinical criteria, they have left out the integrity criterion, and I brought this up at the Standards Committee meeting and they said that—they said that that's because the integrity criterion is written for transactions, which is true, but—and that there was no, were no

criteria in the clinical module that had to do with transactions, but in truth, they, their, they do have, transmissions are involved in the, in the clinical criteria, so we wanted to recommend that they put that in and not leave it out.

Care coordination, as you guys pointed out, amendments can be made in care coordination, so we felt that amendment should be in that, and finally, in the design and performance module, most of that is truly design and performance metrics, but it also includes the criterion about an application programming interface and to be able to query for data, and in that API section, it has security, but I think the only thing it mentions is, like, TLS. And we recommended adding for the API criterion only the authentication, access control and authorization, auditable events and tamper resistance and integrity. And each of those is—1, 2, and 8, they're three security criteria. So, if anybody has anything to add to this, or to a question in the Word document? Next slide, please.

The NPRM proposes to require a health IT module to automatically stop user access to health information after a predetermined period of inactivity, and to require that the user authenticate to resume or regain access, and we suggested a language change to automatically save the session data and terminate access to protected health information after a configurable period of inactivity.

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture**

Say, Dixie, this is Jeff Brandt.

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

Yeah, mm-hmm.

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture**

I have a little bit of concern with the comment “the suggested language,” being that we may want to be more specific on what data we want to save, because session data can be a lot of stuff. So, do you want to talk about, you know, specific entered or changed data?

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

How do you say that? Because you want—it might have been changed—hmm.

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture**

User, user updated—user updated data?

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

You really want them to come back to the same session and in, at the exact spot in that session.

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture**

Well, we're not saying that.

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

I understand how the term session data is a little too broad.

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture**

Yeah, we're not saying that you're gonna return to that session. That's a whole different—

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

Yeah, but you don't want them to, for example, you don't want them to come back and then see on their screen only, you know, a sentence that they were in the middle of saving, for example. You know, you want them to be able to come to their work, the spot in their work where they were.

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture**

Yeah, I wasn't, I wasn't disagreeing, I was just saying that we need to state it differently.

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

I know, I know, I know, but I think if we had changed data, I don't think that's exactly what we do.

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture**

Oh, I see what you're saying. All right, how about—oh, I know the term—

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

Question, what about if we illuminate the data and just said—

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture**

We re-enter, we—the system will automatically re-enter the session where it was left off, in the state that it was left off.

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

Yeah, that's more along the lines of what the industry has for terminology. We open up sessions, we close sessions, we hold sessions.

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

Okay, okay, so we have automatically—let's see. I see.

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

Automatically retain the session and allow the, redirect the user back to that session when they re-enter the site.

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

Yeah, maybe it goes, like, at the end, because what you're really talking about is when they come back. [Laughter] You know, we don't want to dictate how they do it. We want to say they automatically terminate the access to protected health information after a configurable period of inactivity, and enable a user to return to the session after—

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

Its current state.

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

Yeah, yeah. In the—yeah. Is that how it—so, can you give us words?

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

[Laughter]

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

Automatically terminate the access to protected health information after a configurable period of inactivity.

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

And—and redirect the user to the banded session upon re-entering the site.

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

Re-authentication, yeah.

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

Okay.

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

Yeah, I think that's a really, that's a—because the way it's stated, it almost dictates how they do it rather than just saying what they want, what we want.

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

Agreed.

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

Yeah, good point, yeah. Yeah. You got that, Jeremy and Chris?

**Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology**

I think we got it.

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

Great. Okay, next slide, please. Thank you—good point.

The NPRM proposes to update the encryption standard. It's just an update of the standard, right? Next slide.

Okay, so in addition to agreeing with that update, we wanted to suggest adding a reference to FIPS 140-2, Annex A, which already is in the criteria, that we would add the guideline for transport layer security, or TLS, to support the proposed new certification criteria for application access and patient and where it appears—and that application access appears at two places, patient engagement and common clinical data set. It's almost verbatim, it appears at two spots—but basically, we're saying, when they provide the application access that we should reference the FIPS 140-2, Annex A, TLS guideline. Right?

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

Yep.

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

Okay. Next slide, please. Okay, integrity. The NPRM proposes testing against the—right now it doesn't make it clear how you test integrity, and of course, it's difficult to test that you've actually applied the hash at the, when you generate it, it's easier to test at the receiving end than at the sending end, and so that's all they were saying is that we're just gonna test at the receiving end instead of both ends. And they asked us about guidance on when to go to SHA-2. We agreed on the testing approach and we also, this group agreed that it's time to move to SHA-2 and the 2015 edition.

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture**

Say, Dixie—this is Jeff, again.

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

Uh huh—uh huh.

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture**

I have a question about SHA-2. If we're going to do that, then we probably want to talk more—the SHA-2 is much more complex than SHA-1, but you have to have different block sizes and such like SHA-256, 512 and such. Do we want to at least make some kind of a note, because a decision needs to be made on that, on which one we're going to suggest.

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

On block size?

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture**

Yeah, if you look at the, if you look at the SHA citation—

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

That's a negotiation. It happens, though, between the sender and the receiver. When they send up the TLS, they negotiate what to use.

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture**

So you're—you're not gonna make that part of the, the standard that you have to use 256, 512, or SHA—either of those, I'm sorry. There's actually two sets—SHA-224 and 256. I'm looking at the standard right now. I just wanted to know if we're gonna suggest anything there or just leave it open to the two endpoints.

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

What is—what is your thought?

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture**

You know, I'm not an expert on this, exactly, but I know that today, 256 is, is good enough. But as soon as a computer gets fast enough, 512 will be, need to be done. And so the really high, high security,

which I'm not suggesting now, is already going to 1024. So I would think, at a minimum—well, the minimum is 256, which maybe, if we're allowing the endpoints to actually come up with a decision between the two, then it's a moot point that I'm making, I'm trying to make. I just wanted to bring it up as, do we need to do anything, here?

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

I don't think so, because it is part of that negotiation between the two things.

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture**

Okay. We might want to put in a note there that the block size is in negotiation, just so when people see it, they go, "Oh, which one should we do?" Just a thought.

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

So we could say at least 256 if you wanted, [Laughter] because that's the lowest—

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture**

No, I don't mean that, I don't mean that. Does everyone that's reading this know that they have to negotiate those, is that part of the specification that we're showing? That's just my question. Because if I saw this, I'd go, "Oh, which one do we, should we do?" Not, "It's no big deal," but "Which one should we do?" Except, the higher the bits, the slower the rate.

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

Yeah. If I read that and I didn't see anything specified, I would assume it could be 256, though.

**Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture**

As long as it's between the endpoints and that's known, I totally agree. The question I asked when I saw it, I go, "Which one are we using?" [Laughter] So that was—and then I was thinking, "Who should I ask?" So it was just a question from me, so I was wondering, did we need to say anything at this point that allows people, lets people know that it's negotiated between—or refer them to another piece? And maybe it's not even necessary. Does anybody else have a thought on this?

**Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.**

Yeah, this is Brian Freedman. I think that, you know, it's really a policy choice, so you shouldn't have to specify in what we're commenting on.

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

Yeah, that would be my thought, too.

**Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.**

Okay. I just wanted to bring it up, because it was a question.

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

Okay. Okay. Next slide, please.

Data Provenance. They ask us to comment on the maturity and appropriateness of the HL7 implementation guide for tagging of health information and Provenance metadata in connection with the C-CDA and the usefulness of the implementation guide in transitions of care, download transmits—view, download, transmit, et cetera. Our proposed comment is, HL7 Provenance implementation guide specification—specification doesn't need to be there—takes a different approach from that being pursued by the FHIR. There are two efforts in HL7, both focused on data Provenance, which is a very good thing, because that's important, but the FHIR team—which is HL7 as well, both of these are HL7—is based on the world wide web consortium Provenance specification. The HL7 Provenance implementation guide is really based on what's inherent in the C-CDA and DS4P already, so it doesn't go to the W3C, so they're compatible, but they're slightly inconsistent, and they are, the important thing is, there are two efforts within HL7, both addressing Provenance.

So, we want to encourage ONC to follow the development, adoption, and use of both the Provenance IT spec and the FHIR Provenance content specification, because we think both Provenance is important, it's important to follow both of them. But we don't think that either of them is ready to be adopted as a national standard. Any comments?

**Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.**

I agree with you. One of the things that I was always concerned about this, it may not be appropriate here, but I'll just bring it up, is once you get, since we're bringing in all these sensors in the It world, the Provenance from the sensor, I just wonder when that's gonna be addressed—which it's already addressed in 11-073, it's just, it hasn't been mentioned, from what I've seen. And again, I'm not sure if this is the place to bring that up or not.

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

Whether sensor is a Provenance? I'm getting—

**Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.**

Well, sensor is—wherever the data originated is Provenance, so where, if it originated at a sensor level, then have you get it from there, that Provenance back to, let's say, FHIR, which is on a cell phone or something like that, and I think that that bridge of, say, they've not ever mentioned anything about anything lower than strictly a TCP layout or negotiation, Provenance, so if it's going—

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

Yeah, right. We don't know where—

**Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.**

- for the MAC layer [Cross talk]—

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

Yeah, they don't say where it needs to be recorded. It could be recorded in the sensor, it could be recorded at the other end of the TLS link that received it.

**Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.**

So it's the next layer of—

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

Yeah, I'm sorry, this is Jonathan, if I may just comment on that real quick. I think that that is something that is in scope and is being addressed by the Data Provenance S&I Initiative which, I think, goes towards harmonization efforts. We'll be looking at the HL7 CDA, the C-CDA IG as well as the HL7 FHIR specification for Provenance. And I guess a minor point of clarification, which I just got back last night from an HL7 workgroup meeting, and an EHR workgroup that is developing the Provenance FHIR specification in the context of EHR life cycle events is working very closely with the CBCC and Security Workgroups and Structured Docs working group that have sponsored the one that you've been asked to comment on, I guess, the CDA.

So, they—they are working together. There is more work that needs to be done on both. I certainly concur with that. I would, I guess, maybe say that perhaps they're not as far apart from each other as might be perceived if we went back and just listened to the recording from this call. So know that the workgroups are working closely together, but the maturity is certainly not there yet. Even though the maturity of the underlying specs are there, the maturity of this particular overlay certainly hasn't been fully tested yet, and just to cut to the chase, I think encouraging further pilots and work in this area, given that the Standards Committee had previously voted on it as one of their top priorities would make sense.

**Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.**

Thanks for that update.

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

Yeah, that's very useful. Why don't we tweak those first two comments to reflect that. Jeremy?

Kathleen

This is Kathleen. I just wanted to mention that we, in doing this work, we have mapped all the CDA capabilities for Provenance to W3C and it's a perfect match, and that we are working to bring the FHIR1 into the same—up to the same model.

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

Yeah, why don't we, why don't add a comment that we really are supportive of the work that's being done in Data Provenance, but make it clear that those two are, that the HL7 is working on both of these collaboratively and encourage ONC to follow them and to support their piloting. Or maybe there's just gonna be one, I don't know, but we do want to reflect that and commend the work and recognize that they are collaborative efforts between the two. Okay.

**Michelle Consolazio, MPA – FACA Lead/Policy Analyst – Office of the National Coordinator for Health Information Technology**

Dixie, this is Michelle. I just want to note the time. We're getting close to the end.

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

Oh, yeah. Oh—oh, yeah, we are. Let me see. How much, how many more of these do we have? Let's see. We have—let me see, I'll bring it up on my sheet. We had the auditable events, which we've already been through, and then we have—go to slide 19, we've got—well, that's okay, that's our summary. We only had auditable events, which we've already been through. Go to slide 21, please. Yep. Yeah, so we have, the Standards Committee meeting is next Wednesday, the topic for our June meeting hasn't been established yet.

So this has been a really good discussion today, and I really appreciate all of you for dialing in, and I appreciate our guests for joining us today. We really appreciate Bob, Kathleen, and Jonathan—we thank all of you for dialing in and helping us today. So, let's open it up for public comment.

**Michelle Consolazio, MPA – FACA Lead/Policy Analyst – Office of the National Coordinator for Health Information Technology**

Okay, Len, can you please open the lines?

**Public Comment**

**Lonnie Moore – Meetings Coordinator – Altarum Institute**

If you're listening through your computer speakers, you may dial 1-877-705-2976 and press \*1 to be placed in the comment queue. If you're on the telephone and would like to make a public comment, please press \*1 at this time.

There are no comments at this time.

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

Okay. Thank you, all, so much. We really appreciate, really appreciate your participation. Have a good weekend. Bye bye.

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

Thanks, Dixie.

**Michelle Consolazio, MPA – FACA Lead/Policy Analyst – Office of the National Coordinator for Health Information Technology**

Thank you, Dixie.

**Male**

Bye, everybody.