

Privacy & Security Workgroup
Final Transcript
March 22, 2012

Presentation

Mary Jo Deering – ONC – Senior Policy Advisor

Good morning. This is Mary Jo Deering in the Office of the National Coordinator for Health IT. This is a meeting of the HIT Standards Committee Privacy and Security Standards Workgroup. I'll begin by taking a role. Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I'm here.

Mary Jo Deering – ONC – Senior Policy Advisor

Walter Suarez?

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

I'm here.

Mary Jo Deering – ONC – Senior Policy Advisor

Anne Castro? Steve Findley? John Blair?

John Blair – Tacanic IPA – President & CEO

Here.

Mary Jo Deering – ONC – Senior Policy Advisor

Lisa Gallagher?

Lisa Gallagher – HIMSS – Senior Direct of Privacy & Security

Here.

Mary Jo Deering – ONC – Senior Policy Advisor

David McCallie?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Here.

Mary Jo Deering – ONC – Senior Policy Advisor

Wes Rishel? Sharon Terry? John Halamka? John Moehrke?

John Moehrke – Interoperability & Security, GE – Principal Engineer

I'm here.

Mary Jo Deering – ONC – Senior Policy Advisor

Ed Larsen? Mike Davis? Kevin Stein? Chad ...? Staff on the line?

Joy Pritts – ONC – Chief Privacy Officer

Joy Pritts

Will Phelps – ONC – Office of the Chief Privacy Officer

Will Phelps.

Avinash Shanbhag – ONC – Director, NwHIN

Avinash Shanbhag.

Mary Jo Deering – ONC – Senior Policy Advisor

Any other staff on the line? Thank you very much. Back to you, Dixie.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Thank you very much, Mary Jo. Thank you all for dialing in. Thanks for any public who have dialed in as well. We have really only one topic on our agenda today, but I wanted to preview what we have ahead of us once we finish this today.

Today, we're just focusing exclusively on the notice of proposed rulemaking for Standards and Certification criteria. I just noticed my name was misspelled on this slide, double take. So, I don't think—well, we have two hours reserved for this call. I think we will certainly make progress during that time at the very least.

Following that, we're going to undertake, not today, but in followup meetings, the development of test procedures for the certification criteria. This work is being led by the Implementation Workgroup, and they have asked us to do the test procedures for Privacy and Security. So, we're fortunate to have Will Phelps who's on the line today who is with ONC, and Will will be helping us develop those test procedures. He'll be working with NIST to develop some test procedures for us to review and comment on and make recommendations. So, that's what will be our agenda for followup meetings.

Are there any questions? Okay. With that, let's start the review. I only see the Privacy and Security Workgroup grid over here. Do we have the compare? Yes, that's good. This is the compare document. Both of these documents were provided to us by the Office of the National Coordinator. The compare document compares on the right-hand side what the Standards Committee recommended, and on the left-hand side, it says what was proposed in the notice of proposed rulemaking.

I sent to you the entire compare document, but I did highlight those that the Privacy and Security Workgroup had provided input to. Now, I thought that probably the most, certainly the most dispersed across this document and probably the most challenging to really understand and track in the NPRM were the secure transport standards. So, I want to start with those, and those begin on row eleven in this grid that you see right here.

The transport standards—the standards themselves include three standards, the Direct, SSMPPS/MIME, XDR/XDM. I'll show you those as well, but they're further down. The standards here at the bottom are the standards in section 170.202 (a). There are three standards included there although they aren't specified as precisely as they should be, but ONC knows that and is making those corrections.

What they're intended to be is the number one, is the direct protocol SMTPS/MIME. Number two is intended to also be the direct protocol, but the on-ramp, off-ramp for between Direct and other protocols, especially exchange other IEG protocols, XDR and XDM, for direct messaging. That's number two. Number three is the SOAP based secure transport.

So, those are the three standards that were specified. Then, if we go back to eleven, there are two certification criteria that specify that refer to that 702.202. Then, there are also secure transport certification criteria that don't refer to those. So, that's what we'll be discussing first, as you can see. It's a little bit convoluted.

So, the first is there's an electronic download. This section, section eleven, has to do with enabling patients to get to obtain secure messaging with their physicians and also to download a copy of their

electronic record and to request that their record be sent to a third party. So, we have under the patient, this is patient communications, we have electronic download and we have transmit to a third party.

So, here you can see the electronic download. It says it's a file in human readable format that they have to be able to download a file in human readable format, a summary of care record formatted according to the standards that includes as a minimum these topics. Then, the transmit to third party is where they can request that the record be sent to a third party.

The transmit to the third party does reference the standards, one and two, which are both the Direct protocol. So, let's discuss that. Are there any comments about these are the patient communications protocol?

I should go down to the patient messaging and you can see here's the reference to the standard. The other piece of this is direct messaging. Secure messaging, electronic send messages to and receive messages from the patient. In this case, it doesn't refer—isn't restricted to direct, but it does say that it needs to be secure in a manner that ensures both the patient and EHR technology are authenticated and the message is encrypted and integrity protected in accordance with 170.210. So, are there any comments about these secure transport?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Dixie, I'll start off. I'm confused about what the number three standard is, the SOAP based secure transport. The way those standards are written is layered and complicated, and I'm probably just missing something, but what does that actually mean? Is that actually XDR, or is that merely saying that SOAP is an acceptable subsystem to layer other things on top of without specifying what to layer on top of it? How do you read that?

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

I think it's confusing. I think it's intended to be a way for direct—the intent and Steve Posnack has made it really clear, the intent is to specify the use of direct. The first number one is really the direct SMPP. Number two is XDR, XDM, which is that ramp to number three, which is really they're intended to mean the exchange SOAP as in the exchange protocol. John Moehrke wrote a really nice blog about this. John, would you like to add something about that?

John Moehrke – Interoperability & Security, GE – Principal Engineer

Sure, I can. Certainly, my interpretation—the third spec that they're pointing at, the secure SOAP spec, is a spec that has been written since we started this whole S&I framework stuff in re-documenting, and what it is doing is it's extracting out of the ends and exchange specifications, which we looked at before, which were the query that's retrieved as push, all these different pull stuff. What it's pulling out of those is the common piece, which is from SOAP on down.

So, it includes SOAP. It includes SAML. It includes the vocabularies that the NHIN exchange uses for the SOAP and the SAML, and it includes the TLS as the network layer. But you're right, David, and it is somewhat confusing as to given that there's no selection or SOAP response definition, it's not clear if that just simply means any SOAP action and SOAP response that's using that SOAP transport is okay, which of course the NHIN exchange would be fine.

... XDR would be fine, but that is kind of confusing. It would be nice to get some clarification if that was the intent or if that's just a way to interpret it, but it is the specifications of the SOAP layer on down, the common part between XCA, XCPD, XDR and some of these other core transports that are being used in the exchange. So, it is a common piece.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

It was intended to be the reference to those newly structured exchange specifications, but I don't know whether the reference itself is correct or not.

John Moehrke – Interoperability & Security, GE – Principal Engineer

There are some typos, just like there is in the B transport. There are some typos, but I think those are easy to fix.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I agree with the way John read that. so, I'm glad I'm still able to read because it struck me as that that might not have been what they were trying to say, that they might have been actually trying to say XDR as a form of transport for transmit of the patient's record, but that raises the questions of their intent, which seems clear to focus on direct and then a question of what would vendors actually be certified against. Would it be both of them? Is it just any SOAP? Is it something you could contest? It is a model, I think, right now.

John Moehrke – Interoperability & Security, GE – Principal Engineer

Yes. I think that is the crux of the problem as is today. It is unclear what would be required of a certified product. Scalability here becomes a question. Clearly the big vendors, we do all of the above, and it's not a problem, but how do you scale it down to a small vendor? So, I think there's certainly a scalability question.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Dixie, I agree with you that based on Steve's conversations with us at the last full Standards meeting, the intent seems to be to enable direct everywhere, and they've actually sort of bent over backwards to push in that direction, no pun intended. But then, this language in there kind of begs the question of maybe you still have to do all of it anyway and then it gets confusing. So, I don't know—do they want just for us to make a recommendation back to them of what we think it ought to say or just—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes. Point out the issues and make the recommendation. I think the intent where, in my opinion, where it really comes into question is the fact that one certification criterion in one spot requires the third is optional. This is on down here near the back. See, where we have the transmit certification criterion, we have enabled the user to electronically transmit the summary record created in paragraph I, in accordance with the direct standards, which are 170.202 1 and 2, direct and XDR, XDM. Then, they leave the SOAP as optional.

So, I think that that creates confusion as to what products are certified against, which is the point that you guys are making. You'll hear me typing, and Walter and I are recording your comments as we discuss that. So, you want to say the intent is not clear, which brings scalability into question. It's unclear what the SOAP spec is.

John Moehrke – Interoperability & Security, GE – Principal Engineer

If I'm clear—if something like XDR using the C specification would be accessible, I think that is the intent to allow the things that are being done in the NHIN exchange to be considered accessible.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I think that's the intent.

John Moehrke – Interoperability & Security, GE – Principal Engineer

The other comment I would like to get in is this one is here is clear that it's one and two are specified and three is optional, but the previous section doesn't mention three. Now, it does not mentioned, I guess that's just about equivalent to optional, but I think they should be consistent.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, that's a very good point.

John Moehrke – Interoperability & Security, GE – Principal Engineer

That, of course, leads to the question of this is certification criteria. What does that translate into operational criteria?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I agree with John's interpretation that the intent seems to be that the XDR based approach would be an optional approach, but it's specified clearly in one case and unclearly in another case, and it references the wrong standard to back it up either way.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

One point I wanted to confirm from my reading and my interpretation of this discussion is that the standards are not exclusively, exclusively accepting only the use of direct, but rather saying that in order to transmit these messages, whether it's this download or whether it's a CDA or the summary of record, an entity can use the Direct standard or it can use other mechanisms.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

That was something that I was confused personally about initially. We have to remember that these are the certification criteria and standards for the product. They don't say anything about what people must use in real life. Those have to do with the Meaningful Use requirements, but these are to certify a product. So, if you brought in a product that had, for example, Direct and XDR, XDM assuming those are both clarified and also had TLS and REST, the TLS and REST wouldn't be certified, but you could certainly use them in real life. This doesn't exclude using anything. It just says for your product to be certified, it must support Direct and XDR, XDM exchanges, and optionally, it can also support SOAP.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

My interpretation of that was also that except that when I read that Meaningful Use CMS regulation, it points to this standard of the use.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

We aren't reviewing that.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

I know, but, Dixie, what I'm saying is where the circle closes is in the Meaningful Use regulation from CMS where their requirement is to use this standard.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, the requirement—to get your reimbursement and to attest that you are using Direct, but you don't attest that you're not using anything else.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

But you have to attest that you're using Direct.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Right.

John Moehrke – Interoperability & Security, GE – Principal Engineer

You have to count statistics only for where you're using an approved transport. That's a question.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

What?

John Moehrke – Interoperability & Security, GE – Principal Engineer

If you can count in your statistics of patient engagement where you have used this restful interface, then that's not a problem, but if you can't count those because they're not using the official transports, that becomes a problem.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Well, keep in mind, I think that—this transmit to third party, yes, requires restful. Electronic download does not and neither does secure messaging with patients. It does not require Direct.

John Moehrke – Interoperability & Security, GE – Principal Engineer

That one there I read as quite nicely open portals and such.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I thought so too. For the real messaging and download with patients, they don't specify Direct. They specify Direct only for transmission to third party and for the summary at 16.

M

Right, provider to provider.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, this one, transmit to summary of care. So, those are the only two where they specify that the certification criteria or that you must use Direct in the certification.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

It seems like we've got three categories of circumstances. One is what will the vendor have to certify against, and we've clarified that that's unclear. Then, number two is what do they have to actually use to get credit for. That's off the table for today, but that's the Meaningful Use. Then, number three is sort of a vague category of what are they allowed to use from a point of view that it's considered secure and acceptable even if it's in fact not part of the certification tests nor is it something that they get credit for.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Right. I think that third one—that third one is where I personally have a problem with this number eleven. If you look here, this download—for download, there are no security requirements at all.

John Moehrke – Interoperability & Security, GE – Principal Engineer

Security requirements are inside of the standards.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, but not for download. For messaging, they are, but I don't think—maybe they are. Can you point them to me?

John Moehrke – Interoperability & Security, GE – Principal Engineer

The transports? So, the Direct Project has embedded—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

No, this has nothing to do with Direct. Look at B right here. I have on the screen download. This does not require Direct, not for downloads. Transmit for third party, it does. That makes it clear. For download, I don't believe, and for messaging, it also says it

M

Good point. They should be specifying something there.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

For secure messaging, they clearly specify encryption and hashing and authentication, right?

John Moehrke – Interoperability & Security, GE – Principal Engineer

True.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

If you leave it open to use TLS or whatever, but for download, I couldn't find anything where they said it had to be secured.

M

Dixie, I thought the preamble on downloads said that common mechanisms are in such common use that they didn't need to specify it.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

First of all, the preamble's not part of the law, but secondly, there's no requirement here for secure. Download, electronically download, it doesn't even—there's no requirement there that I can see.

M

I understand that, but the preamble explained why there's no requirement there. They didn't think it was necessary because common use and other constraints like HIPAA would cause it—

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

That's this one. That has to do with this one. This one is where the preamble brings that in is the secure messaging. It doesn't bring it in for the download.

M

I think what David's point is they have said it is so common, it's not necessary for them to spend federal dollars on ink.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

I agree for this one because it has secure there. It has it in the requirement. It has to be authenticated. It has to be encrypted and integrity protected. So, I agree. You don't have to go into TLS. We know how that's generally done. But if you look at eleven, it doesn't say anything about authentication, encryption, integrity protection or anything. It just says downloaded.

M

So, what you're saying is you would like to add the

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Exactly. I would like to see the same two apply to electronic downloads, that it has to be authenticated, integrity protected and encrypted.

M

And, Dixie, what do you mean by encrypted?

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

I would like to see ... electronic download here, you can see where I'm point right?

M

No.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

I would like to see exactly the same words as I see for messaging. What I see for messaging is that any manner that ensures that the patient and EHR technology are authenticated, the content is encrypted and integrity protected, exactly those same words. I would like to see for downloads.

M

So, on the download question, does that mean that the payload is encrypted or that the channel is encrypted? In other words, if I use HTTPS—

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

The channel because you want to also encrypt when they log on.

M

But are you requiring that the actual document that's downloaded

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

That's a good point. In my opinion, it should be the channel because you want to encrypt their past ... authentication information as well as the download.

M

So, really, you probably want to put it above then at the I level.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

At the I level?

M

Which is I is what's introducing the—

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

I know what you mean. The whole—

M

Which actually C is related to I. So, I think C relates to any part of I. So, I is the ability to gain online access—

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Yes, I agree with you, right here—

M

I think it's in there already, Dixie.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Well, we have I is enable, A is view. So, we don't require security to view. Then, download and we don't require security there either. Then, we come to C, transmit to third party, and we say, yes, that has to be secured. Here's II.

M

You would want the portal viewing to be secure.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

I know. You'd want them to log in for that as well.

M

Yes. So, you kind of want to apply the same clauses we have down on line 14.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Yes. John, what's above I? What is this a part of? Maybe it's like the level above I.

John Moehrke – Interoperability & Security. GE – Principal Engineer

That's actually

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Because I is online access. II is log. What's III? II, there's no I. I think they cut something out here.

M

Yes, whenever you put it into a spreadsheet, you'll end up losing

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

I wonder how much we—

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Maybe our comment is that we believe that all interactions with the patient need to be secured and the requirements don't apply to all of it.

M

Yes, following that same spec that we have—and that's the question is maybe they have closed the loop and we just don't see it because it's in the spreadsheet form.

Joy

Dixie, this is Joy. I'm going to see if I can find the entire text for you, okay?

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

That would be great, and then, we can look—I think ... interaction ...

Joy Pritts – ONC, Chief Privacy Officer

I know you've been talking about—that screen open. Can you give me that first number on it so we can track it down?

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

Actually, it's on page 13,883 middle column, the bottom. So, this is the—it's really not on I necessarily. It's more part of the patient engagement. So, this is part of letter E, patient engagement, and then number one is view, download and transmit to third party.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

So, E is above here.

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

E is above the participation engagement. So, this is really kind of the categories or the domains, high-level domains.

John Moehrke – Interoperability & Security. GE – Principal Engineer

So, E is patient engagement. I is view and download and then one.

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

Really one, and then I.

John Moehrke – Interoperability & Security. GE – Principal Engineer

There's really nothing before that. So, really, yes, we probably could insert that electronic patient engagement should have the same security criteria.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Well, but it's certainly why they didn't do that, John, is because they want C, transmit to third party, to be Direct, but they don't necessarily want messaging and download to be Direct, which is right.

John Moehrke – Interoperability & Security. GE – Principal Engineer

That's fine though. The other clause down below in our spreadsheet, row 14, that's just talking about interacting with the patient using secure technology and the way they write that, a portal mechanism is sufficient.

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

I think those two clauses on 14 can—

John Moehrke – Interoperability & Security. GE – Principal Engineer

I'm just wondering if that is already tied and we just don't see it in this format. But messaging is not the same as download.

John Moehrke – Interoperability & Security, GE – Principal Engineer

Correct.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Secure messaging is interactive. I think they've covered messaging. I think they've covered transmit to third party. I don't think they've covered download.

M

Or view.

John Moehrke – Interoperability & Security, GE – Principal Engineer

I think it would be interactive. Any of the online interactions should also have that same clause, which simple HTTPS seems to go with, and that's what everybody's using so it's not like they're asking for something that's not in play.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

So, we're saying every online interaction, whether it's between two providers or between provider and patient or whoever else, should have the two clauses on row 14.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, but this whole section is about patient interaction.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

I understand, but I'm just saying—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, viewing and download as well as the other interactions, and a transmit to third party is really a request from that patient. Okay, I think we've captured that, and Walter and I will wordsmith it and run it by you guys. Okay?

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

Sounds good.

John Moehrke – Interoperability & Security, GE – Principal Engineer

Yes, I'm okay.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Okay. Let's go onto the meaning of our—now, how this relates to our recommendations is we never specified Direct. We did specify SMTP and TRS and S/MINE and then the NCRM had moved it to Direct. Okay. These are line 20, which I have on the screen right now, this is authentication, access control and authorization. What we recommended was ASTM 198.609 for access privileges but note the—and we recommended words for both person authentication and entity authentication, and we recommended NIST 80063 level two for single sector authentication and ITU X509 for digital certificates. What the proposed criteria are to verify against a unique identifier using name or number that a person seeking access to electronic health information is the one claimed and establish the type of access to electronic health information or users permitted based on the unique identifiers provided in C1-I and actions the users permitted to perform with the EHR technology.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

So, here they're really not recommending a standard but some certification procedures.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Well, they ... standards, just like HIPAA does. That's the standard is what we described, and they may or may not reference an SDO.

John Moehrke – Interoperability & Security. GE – Principal Engineer

Once you put something into regulation, it now becomes a regulated—hindered by regulations. In the preamble, they do explain that they feel authentication technologies are pretty common and they didn't need to drive any specific things. That's probably true, especially when interacting in this way.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

It's important to know though, once these regulations are really codified, the preamble is not part of the law. It's explanatory when it comes out, but it's not in the law itself once it actually gets in the law.

John Moehrke – Interoperability & Security. GE – Principal Engineer

Correct, but what they're saying is having said nothing in the law isn't going to cause bad things to happen.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

I agree. I think the one part that we recommended that they didn't include, personally, I think it is an oversight because they addressed only person authentication that a person seeking access to electronic health information to win claims, and we recommended that there be separate person authentication and entity authentication because you want to authenticate servers as well as people.

John Moehrke – Interoperability & Security. GE – Principal Engineer

I made that observation as well, is that they missed that machine should be authenticated by X509 and I think that was because they ... intended that everybody should get a X509 cert, and I don't think that was necessarily part of the plan, but at least where the technology supports, and this would actually include S/MIME, but where the technology supports certificates, certificates should be used.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Yes, I think that that's—I would agree both of those points should be made.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

In an attempt to keep the law as simple as possible, aren't these essentially covered under addressable HIPAA issues by status quo? Are we adding any value by putting machine authentication in here?

John Moehrke – Interoperability & Security. GE – Principal Engineer

By that measure, David, and I can go down that measure, then we shouldn't be specifying an encryption rhythm or a hashing rhythm because they're also just as covered. I just see a non-symmetry. They're specifying that you must go to HIST for your encryption algorithm and for your hashing algorithm but they give you no guidance on what you should do for your authentication algorithm.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

David, keep in mind, HIPAA is for organization. HIPAA is what organizations must do. This is what a product must do.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Right, but in order for—

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Pardon?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I understand. This is a rule about certification, but in order for the product to actually get any use in the real world, it's going to have to meet existing standards.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Maybe X509 is part of Direct, and they felt they had it covered.

John Moehrke – Interoperability & Security. GE – Principal Engineer

Well, ultimately, it is part of Direct. It is part of the XDR, XDM, and it is part of the SOAP, but so is AES and so is SHA. So, why specify one, those two, and not the third? So, either go all in or go all out. Asymmetry in the regulation is what will cause problems, and I'll tell you in Meaningful Use stage one, it's absolutely caused poor designs to actually make it all the way through certification.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

That's what we just talked about too. If we add that viewing and downloading need to be secure, those are going to be secured with X509 certificates using TLS.

M

....

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

I think we should suggest they add this. Both of the things, both ND authentication and what John says that X509 for authentication whenever is appropriate.

M

How would you certify entity authentication? That's so broad.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

How would you do what?

M

How would you certify that someone is doing entity authentication? That seems broad.

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

This is about certifying that an EHR has the ability of doing NTP authentication.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

So, when it connects to a server, it authenticates the server, or when it sends something to another provider, it authenticates the provider.

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

This is where, again, the question becomes, okay, the EHR might be certified to support X.509, then the question is will the provider be required to use it, and that's where the HIPAA security regulation might come in by saying well, now that the EHR technology is common in the marketplace to support X.509, you must turn on that in your systems.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

But I think he's asking how would you really test that product uses X509 all the time or is able to use X509 to authenticate any entity it connects with?

John Moehrke – Interoperability & Security. GE – Principal Engineer

Well, you're going to have the same problem with the ... encryptions and the ... so again, we have— symmetry is all I'm asking for.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, and I'm with you, John, on the symmetry point and I would probably push to reduce the complexity rather than the increase the specificity because I'm just concerned that entity authentication can occur in a variety of different ways, some of which aren't 509 based. There are other approaches that are equally secure and may be perfectly appropriate for certain kinds of interfaces. I just wonder if we get into more trouble by listing a vague goal that really can't be tested given that its use is already regulated.

When it comes to the transport connecting—well never mind. I'm repeating myself. I guess the point about the asymmetry, and I think it's an issue. I just don't want to make it more specific. I'd rather make it less.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

So, David, you arguing for a statement like the one we have recommended on entity authentication is to broaden not testable, or are you arguing for the fact that if we insert the statement about entity authentication on recommend the use of the standard X509, that's too much specificity?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

The latter is what I'm worried about. I don't have great language to suggest. If I had a piece of text, I'd suggest it. I just worry about locking in on something that might not, in fact, be a standard in four or five years. It might not be the only way to do things in four or five years, and yet, we have equally secure—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

But do you agree that we should add entity authentication but you just don't want the X509? I want to be clear.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Good question, and I'm confused. So, if my answer is inconsistent, it's because I haven't got it settled in my head yet. I think personal authentication is very clear what that means. Entity authentication is not nearly as clear, and I'm concerned about introducing a vague notion of entity authentication. As a principle, I think we all understand what it means. As something that's testable, I'm not sure how to test it. I can test that you authenticate for login of users. That's easy. We do that already in Stage One.

I'm not sure how to test for entity authentication. On the other hand, the specific entity-to-entity exchange mechanisms that we've discussed for download and messaging and the like, we've got that well covered. Those are all based on standards that use TLS and 509 and other things. So, I'm just not sure that adding entity here helps as much.

John Moehrke – Interoperability & Security, GE – Principal Engineer

So, essentially, within the three defined transports, since they already include the authentication, the encryption and the hashing mechanisms, beyond those is the place that gets foggy, right?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Right. So, we have somebody connected to Surescripts or somebody's connection to a lab interface.

John Moehrke – Interoperability & Security, GE – Principal Engineer

So, it's the unintended consequences of saying a generic all systems shall be authenticated by X509, and it's true that when you look at some of the ways in which Surescripts interfaces are done, they're done through a VPM link, which may or may not be using X509, and does that then make them completely invalid? They do have an X509

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Entities, though. Even if you use a VPM that uses password authentication, you still are authenticating the entities. I can't even imagine that we wouldn't have a requirement that every entity that you exchange information with has to be authenticated. Even if you have a VPM there still, an IP VPM, they still authenticate each other.

John Moehrke – Interoperability & Security, GE – Principal Engineer

Yes, but I'm kind of heading more towards I think where David is, and that is that standard practice today already does the right thing. So, I think we should only be specifying where today's practice is misguided or what have you.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

But we don't need any of this is we would say okay, everybody's doing the right thing so we don't need any rules, we wouldn't have any of this. But they aren't doing it right and ... the right thing.

John Moehrke – Interoperability & Security. GE – Principal Engineer

I think what the law is doing here or the regulations, they are being precise about new capabilities and XDR and Direct to be new capabilities not yet in widespread use, but not necessarily reregulating things that are already in widespread and appropriate use, particularly when it comes to the point of certification.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Technology has people log in already. I agree with you that we don't want to lock in X509 because next week we might have something different, and I also agree with John, that some IT sec VPNs don't use X509 authentication. But I do think that we need to include entity authentication there. I think this is important in person authentication and just as I think it's less widespread than person authentication, quite frankly. Routine practice, I think, person authentication, is much more a routine practice than entity authentication.

John Moehrke – Interoperability & Security. GE – Principal Engineer

How would you test it?

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Well, you test whenever—every time the interface that allows the exchange of health information would have to authenticate the entity at the other end before it's sent information.

John Moehrke – Interoperability & Security. GE – Principal Engineer

So, let's walk through the scenarios. I think where the testing, the certification testing is doing anyone of the three transports, that's not a problem. I think that's—so, the question then becomes how else would you prove that there's no way that the EHR technology can communicate except through an authenticated link? I think that becomes the infinity problem.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Well, you could do it with TLS between—

John Moehrke – Interoperability & Security. GE – Principal Engineer

How would you test that there are no other ways? You're talking about the no problem.

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

But do you really test for the no problem? Or do you just test for what is expected to be supported by the EHR?

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Right. If you've got a—

John Moehrke – Interoperability & Security. GE – Principal Engineer

If you test Direct, XDR, XDM, the three defined transports, then—

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

But there could be others. Those are the three that they must have.

John Moehrke – Interoperability & Security. GE – Principal Engineer

That's the problem that we're arguing. What is the it could be others? How are the certifying bodies going to discover what the it could be others are?

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

I don't know that they have to discover that there could be others. They just have to confirm that the EHR supports at least one of those three transports so that when the provider uses that EHR and is expected

to conduct entity authentication, the EHR has one or two or three users, depending on which ones they support, to do it.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

But if they use one of those, then I'm not worried about entity authentication because they're already taken care of. But if they use—like Surescripts has a different—it's not one of those three. That's a different connection, and I would want to know what are the different ways—and they might have a REST interface, let's say, and I would know fine. A REST interface is perfectly fine, but how do you authenticate the other end of that interface?

John Moehrke – Interoperability & Security, GE – Principal Engineer

Right. That's the piece that's uncomfortable. I would agree with David.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think, Dixie, anyone who's actually implementing those interfaces would of course worry about that because that's best practice. It's also HIPAA, but I'm not sure it's relevant to certifying against an as yet unspecified future potential interface. In order to pass certification, they're going to have to demonstrate that they can do Direct, and they're going to have to demonstrate that they can do SOAP, maybe, if we clarify optional question here, and they're going to demonstrate TLS.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

No, they don't have to demonstrate TLS. That's not in there.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

But it is in the view and download. We're recommending that we put it in there.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

No, we don't have—

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

That's what we would want to recommend.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

If we add it there—

David McCallie – Cerner Corporation – Vice President of Medical Informatics

We're adding it there

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

We're adding it there. You're right. So, are there others? Maybe not. So, do we want to capture—I don't want to harp on this forever. Do we want to capture John's point about the importance of being consistent, or do we want to just leave this one alone? Whatever you want is fine with me.

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

I would say that John's point about being symmetrical is a very important one. That is separate from the other question, which is we're not recommending adding entity authentication, I suppose. So, there are two things about comments in this particular part. One is the symmetry of—

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

That has to do with entity authentication.

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

Is it the same because I thought symmetry applies to other things, not just entity authentication?

John Moehrke – Interoperability & Security, GE – Principal Engineer

Well, that's the piece I'm worried about. They're specifying encryption. They're specifying hashing, but they don't specify the authentication. I have seen in certification for Meaningful Use Stage One systems that got through certification because they could properly encrypt. They could properly hash, but they used a sixth key that was coded into the user interface. That's because no specification for key management is given.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

But you aren't recommending that we add anything, right?

John Moehrke – Interoperability & Security, GE – Principal Engineer

Well, there are two different places in the specification where these things are called for. I think if a defined three transports, the push transports, I don't think we need to say anything about encryption, hashing or authentication because it's built into the specifications, and the specifications can properly handle it there. The other place is where they're defining this human patient interaction, so usually it's going to be done through some kind of a portal, might be done through an EHR, and there, they are specifying encryption and hashing, but they're not specifying a team management.

So, the question is can we feel confident that HTTPS is used with portals today, and therefore, we don't have to specify encryption or hashing. Or are we so concerned that HTTPS is not used today that we have to specify encryption and hashing and if we don't specify authentication, we may end up with somebody coding their own key management with some kind of an encrypted and hashed interface? It's kind of ... strange either way.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes. The point about X509 being replaced in the future, X509 is already in the transports that they have specified.

John Moehrke – Interoperability & Security, GE – Principal Engineer

I doubt X509 is going to be replaced in the future.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

In the near future, right.

John Moehrke – Interoperability & Security, GE – Principal Engineer

But I think the point David was making is there are interfaces, not human interfaces, machine-to-machine interfaces that are encrypted by a VPN with a pre-shared key, and those shouldn't become invalidated by an inappropriately-placed criteria. So, if we place the criteria in the, I'm going to call it the portal, I'm not seeing it on the screen, and I changed my own copy, but the place where it's patient interaction, we should probably just put something—all interactions with the patient over the internet shall be secured using common technology.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

John, to that point, I opened up the HIPAA regulations because I needed to really see the wording of this, and let me read you very quickly what it reads for personal entity authentication. It says it's a required implementation specification not addressable, and it says implement procedures to verify a person or entity seeking accurate or electronic ... information is the one claimed. I'm not sure that the wording that we have, either on entity authentication or even on the actual recommendation or actual the proposed language for verifying against a unique identifier or established, I don't think that adds anything new. I think that part that adds new things is the thing that you said at the very end of your statement, which was with the following or using the following standards.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

What you just read is different from what's in the NPRM, Walter. What HIPAA says is that the person or entity seeking access is the one to be authenticated. This says a person. It doesn't say anything about entity.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

Well, no, I'm just saying even if we add the entity part, the wording in HIPAA is already the same. When you read the wording in HIPAA, it's saying the same thing as the wording we're suggesting or the wording that exists.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Except that HIPAA mentions entity and this doesn't. That's the whole point.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

Yes. So, let's assume that we add entity authentication where we say EHR technology is not authenticated and identify over certain entities, how different is that from the verify that a person or entity seeking access is ...?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

It's no different. The point is what we are looking at isn't even consistent with HIPAA because it doesn't address entity.

M

Remember this exists—

John Moehrke – Interoperability & Security, GE – Principal Engineer

Well, HIPAA says person or entity. So, if you authenticate a person, you don't have to authenticate the entity.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

What it says now is person.

John Moehrke – Interoperability & Security, GE – Principal Engineer

Right because this you know that you have to do a person authentication. This is drilled down into a workflow where you know you have to do person and doing the entity also in the interactive session isn't all that helpful but especially now that there's a mandate.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

This is a certification standard rather than HIPAA, which is a used standard or requirement. So, I think the question is, to me, is there something that we can certify and test that should be here? We know that in a world of use, HIPAA covers it already, but is there something specific that should be tested in order to get the token that you're a certified EHR?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Maybe once we fix the patient interaction one in between that and the Direct and the transport, we'll have it covered.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think so.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Okay. Let's move on. Auditable events, 21, the auditable events, what we recommended is to detect and record auditable events, must be able to detect and record and to protect audit information. They pretty much incorporated what we recommended.

They did add the enabled by default that auditable, I guess auditing, auditing must be enabled by default, turned on and must only be permitted to be disabled by a limited set of individual users, record actions, record actions to electronic health information actions related to electronic health information, audit log status and as applicable encryption of end user devices. Audit log protection and detection detect the alteration of audit logs. The standard specifies, so here's the standard of what must be audited when the

EHR technology is used, I'm not going to read through all this, audit log is enabled or disabled and encryption of electronic health information on end user devices. Comments?

John Moehrke – Interoperability & Security, GE – Principal Engineer

Well, the one comment I've observed is the All, the audit log protection, is well intentioned, but quite honestly, a possible reality is audit logs need to be purged at some point. They are forbidding in audit logs ever be purged. We can't have audit logs just always grow and never be allowed to be looked at and said yes, we've mined everything we can out of those audit logs. It is no longer useful to keep around and we purge it. Yes, that is an authorized event, but it's pretty common—

David McCallie – Cerner Corporation – Vice President of Medical Informatics

This is David. John, that's a great point. I hadn't thought about that, but is there not a legal requirement of retention from at least some period of time?

M

Yes, but it's not infinity.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I agree. It's not infinity, but—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

We capture that in what we recommend that it would allow audit logs being purged after the required period of retention time.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, that is what I was going to suggest is just refer the notion of a legal retention period, which is probably site specific and state specific even maybe.

John Moehrke – Interoperability & Security, GE – Principal Engineer

It is, yes. I think their intention for that whole line is that entries can't be individually changed, overwritten or deleted, but by the way they write it, it doesn't allow for the audit log as a concept to be purged. So, I think if we just made it clear that functionally analyzing an audit log and purging it is something that is pretty common in audit analysis.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

And they do say actions, actions recorded. So, they sort of imply that but not exactly. We'll just give them their comment and they can make sure that that's The other comment that I had is this first one that I think they've got some operational context in there that they shouldn't have. Where it says must only be permitted to be disabled and re-enabled by a limited set of individual users, the technology shouldn't have to deal with whether the set is limited or not. I think the technology ... know that there's a particular role that's allowed to do that and know of the role.

John Moehrke – Interoperability & Security, GE – Principal Engineer

Yes. I don't think they intended it to be read the way you did, but I think if you just remove the word limited instead of authorized The other part of that, which is also I've seen troubling is if the technology is always recording in the audit but the operation doesn't know that the audit log is there, that can create problems both technically and legally. So, essentially, the technology, the EHR, can add a liability to an organization that they may not be aware of because the technology is using the audit log. So, it's okay but we would have to recognize that that can create an operational liability that the providers need to know about.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

So, is that a comment that we need to—

John Moehrke – Interoperability & Security, GE – Principal Engineer

I'm not sure if we want to change anything or not, but, Dixie, do you know what I mean?

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Yes.

John Moehrke – Interoperability & Security. GE – Principal Engineer

There have been cases where an organization was found liable because the technology they had had recorded events that should have been acted on, but they didn't know that the audit log was there, and that was not considered an excuse. I'm sorry, David. I talked over you.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

No, that's fine. I interrupted you. I was going to say I think that's kind of the point here is the audit log is actually intended to play that role.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Well, are you suggesting, John, that—what are you suggesting?

John Moehrke – Interoperability & Security. GE – Principal Engineer

Well, we need to make sure that in the CMS role, that there is as clear of a requirement there that they analyze all the audit logs provided by the certified technology.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

But I don't think that's part of this.

John Moehrke – Interoperability & Security. GE – Principal Engineer

No, it's not part of this. That's why I said—

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

It's a very good point, but you want to get to any particular comment.

John Moehrke – Interoperability & Security. GE – Principal Engineer

I'm not sure that it's of any use to change this rule. The question people will come up with is to what capability is the audit log automatically enabled, all events, or is there some reasonable set of events that are the—

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

That's what's down here at the bottom. The standard has the event.

John Moehrke – Interoperability & Security. GE – Principal Engineer

So, all of those?

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Yes. The following information must be recorded—when the technology is used to record, create, change, access or delete the electronic health information, the following information must be recorded.

John Moehrke – Interoperability & Security. GE – Principal Engineer

So, a audit system, will create a new audit entry for every character that's changed—

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Yes. When a record is opened, and you know how operating systems—

John Moehrke – Interoperability & Security. GE – Principal Engineer

No, it's the changed one that's

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Open ... changes made and it's closed, it would record that.

John Moehrke – Interoperability & Security, GE – Principal Engineer

I'm just trying to be a devil's advocate here to see how bad could somebody screw this up.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

You know how electronic records, a doctor can be recording something and not commit it to the EHR, write it over a couple of days, a couple of hours or whatever. I would question how that—because you do have a draft. They'll have a draft that they're working on, and then ultimately, they'll say okay, commit this to the EHR. I don't think that this may not capture that aspect of routine operations actually.

John Moehrke – Interoperability & Security, GE – Principal Engineer

That's one of the advantages of pointing at a standard, even if it is the ASTM standard. The ASTM standard clarifies that but because they refuse to point at the ASTM standard, people have to reinvent it. I would like us to re-recommend that they point at the ASTM standard.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

That's what we said.

John Moehrke – Interoperability & Security, GE – Principal Engineer

Obviously, I would love to point at ATNA, but I'm perfectly happy to start with let's at least point at ASTM because that is a ... standard that's framed, what is the concept.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, it recognizes how health care works.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

They did acknowledge in the preamble about the ASTM as one but not limited to type of specification, but they didn't put it in the rule itself.

John Moehrke – Interoperability & Security, GE – Principal Engineer

They could replace all of the text with just compliant list A2147.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

So, you think A2147 would take care of the standard as it's being written in the regulation?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, it's designed for health care actually.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

Because I really like that concept mostly because what is happening here and in other places is that the rule is creating a standard. It's not an external body expert in standards that create the standard and the industry maintains it. It's now a regulation that this is the standard. That is contrary to any—it would be like in the HIPAA world, in the transaction standard saying the way you send a claim or you process a claim is this and you put it in the regulation instead of using X12 standard.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

So, do we want to just say we recommend—now, there's two lists in 2147. There's one for audit and one for disclosure so we would want to specifically refer to the audit piece of it, but do we want to just say we would prefer that it be using that one, ASTM?

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

I would recommend that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think it's important to clarify why we're saying that. I think John's points about the vagueness of some word-like change could lead to implementations that created completely unworkable systems. It defeated

the purpose of logs. So, clarifying the granularity of change that should be captured is an important operational and scalability issue.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

I think the other point is really this point about ability to reference an external standard rather than create it in regulation the standards itself because now anytime there's a need to add one additional data element besides the five or the two that are listed in this, now you have to go to regulations and say now roman number VI will be whatever.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Okay. Let's go to the next one. I've typed that in.

John Moehrke – Interoperability & Security, GE – Principal Engineer

Dixie, before we move onto the next one—maybe this is the next one. I wanted to ask about providing patient access to this log. At one point, there's a requirement that the patient be given access to the person, consumer gets access to the activities of view, download and transmit. Is there any confusion that that might be the same or not the same as the logs that we're talking about here?

M

That's 202A.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

That was back in earlier part, right? Do you happen to know which row? I think that was in those patient things, right?

John Moehrke – Interoperability & Security, GE – Principal Engineer

It's under 202A, below the ..., it was II.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Exactly. The patient acceptable log, is that something different from the ASTM log that we were just talking about or is it the same? Is it a subset? Do we care?

John Moehrke – Interoperability & Security, GE – Principal Engineer

It certainly is not the same because the audit log is all events, and you only want to give the patients access to events that are relevant to them.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

The way this is written, it's really, this log is of activities on what we call here, the portals. See, when the health information is viewed, downloaded or transmitted to a third party, these are activities on the portals.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

That's how I read it. I just was unclear. Somebody was asking me at some point about whether the intent was that this is the patient's view into—this is accountability for disclosures essentially. Is this the place where accountability for disclosures occurs?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

That's accounting of disclosures. That's still an optional one.

John Moehrke – Interoperability & Security, GE – Principal Engineer

This is certainly leading to an accounting of disclosures, but it's saying the transmits seen above are in scope, ... accounting of disclosures.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

But typically, ... is really making the accounting of disclosure of report accessible online.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

No, what we're looking at now is this is a log of the activities that happened on the portal. This isn't about log disclosures or an audit trail.

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

Not just on the portal but transmitted to a third party means not just through the portal.

John Moehrke – Interoperability & Security. GE – Principal Engineer

I think this is—

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Using the capabilities included in ..., now they're trying to limit this to these interactions with patients. Later, we'll get to the ... disclosures.

John Moehrke – Interoperability & Security. GE – Principal Engineer

No, at the very right-hand side of that, it says A through C. C is transmit to third parties.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

This is that high-tech requirement that a patient requests that something be transmitted to the third party.

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

No, but it says when an electronic health information is transmitted to a third party.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Yes, it does say that.

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

Then, you'll have to record all this and make this information available online. Now, that's the online part.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

I think that's confusing because I think what—you know how high tech says that patients have to be able to download electronically or request that their information be transmitted to a third party, I think that's what this is. I don't think this is complete accounting of all disclosures.

John Moehrke – Interoperability & Security. GE – Principal Engineer

It's not clear. The beginning part of the II-A clause could certainly be interpreted as all views, downloads or transmissions inside of the EHR.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

I think we should point that out because I don't think that's the intent.

John Moehrke – Interoperability & Security. GE – Principal Engineer

Which is actually the way I read it. I read it as we're setting up the health care provider to give the patient the high-tech access logs.

John Blair – Tacanic IPA – President & CEO

This is John Blair. That's how I read it too.

John Moehrke – Interoperability & Security. GE – Principal Engineer

I saw this as enabling the patient to get their access log.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

I think that's a really good point to make because I just connected it because all of these are all in high tech. So, I thought that's all it meant. Later, we'll come up with accounting disclosures, and I thought that that's what—yes, good catch.

John Moehrke – Interoperability & Security, GE – Principal Engineer

If that is indeed an access log, then the ASTMs, the second part of that ASTM is applicable without having to restate the ... that is stated above.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

There's a second section about accounting of disclosures.

John Moehrke – Interoperability & Security, GE – Principal Engineer

Was there?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Okay. So, we're recommending ASTM auditing, audit reports.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

What about the other report? We also said ASTM. Should that be replaced as well?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

What? Where?

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

The next one, the 2010.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, we're just moving to this one. We really haven't discussed this one. This is the audit reporting, enable a user to create an audit report for a period of time and sort entries, and what we recommended was generate audit reports for specified time and we recommended ASTM again here. Do we want to do the same thing, recommend ASTM here too?

M

I do.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Who are the users that are being referred to here in number 22? This is EHR users?

John Moehrke – Interoperability & Security, GE – Principal Engineer

Yes, this is a core EHR criteria. So, in section 210 where all of the other core EHR technologies are.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Got it.

John Moehrke – Interoperability & Security, GE – Principal Engineer

So, this is the EHR—they're really just getting a little bit more explicit about the audit, what is auditable, what does an audit log contain, and I think you could collapse all of that and just say following the ASTM E21 standard because otherwise they're just restating and they're restating in such a short form that there will be misinterpretations.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

Again, I hate to bring it up but I lived in HIPAA for so many years, the weakest problem is when you close this into regulations, now the standard is the rule. It's not an external ASTM or X12 or HL7 or ISO that is maintained and updated and all that, but now is some rule that says I have to follow exactly this. That's a big problem.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Okay. So, we're going to say again for low 20 to use ASTM. They wrote 20—this is amendment. Row 23 has to do with amendments. What we recommended was to provide the capability to amend health information while preserving the integrity capability to attach health information, patient asserted information and provider's formal rebuttal and an EHR must maintain an audit trail.

They pretty much recommended what we recommended, enable a user to electronically amend a patient's health record to replace existing information in a way that preserves the original information, which is what we said. Append patient supplied information and pretext or scanned directly to the patient's health record or by embedding an electronic link, enabled to use it to electronically append and response to patient supplied information. Comments?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Dixie, remember on the Tiger Team call, there was quite a bit of debate starting up around that question of free text or scanned. Do you want to touch that, or is that really more of an Implementation Workgroup question?

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

We'll bring it up. The other people weren't on that call

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I'm trying to remember the exact details of that. I think the Tiger Team was concerned about the—I guess there was a question of whether it should be free text and scanned, meaning that you would be required to support the ability to capture a scanned amendment, say, for example, a patient's letter or a handwritten note or something. I'm not exactly quite sure why we got into the deep discussion about it now that I think about it.

M

Well, you can imagine the EHR—yes, we're way off of Security and Privacy, but you can imagine an EHR that doesn't have the ability to have a scanned image as an attachment. It only is a database. Well, I can put free text into a database. That's easy.

John Moehrke – Interoperability & Security. GE – Principal Engineer

I don't know if that was the problem. I actually ... on what is an embedded electronic link? A link to where? A link to a document on the patient's laptop? I'm sorry, but that doesn't make sense.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Well, John, it links—whenever you're reaching out like that, that link can link to something else in the future.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I interpret that to mean a connectable point or not an URL link, but you might, for example, the document displays with annotation that says this document has been amended. Click here to read the amendment, but I agree it's pretty vague.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

It's probably a link within the EHR maybe.

John Moehrke – Interoperability & Security. GE – Principal Engineer

Well, it may be a link within the Health Information Exchange. To David's point, if you have a PHR that is a participant in your health information exchange and the PHR has published a document, you could refer to it by its unique ID. But that's putting together a lot of conditions that just simply saying that an electronic link doesn't necessarily encapsulate, but I get it if that's the point.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Do we want to say anything about it?

John Moehrke – Interoperability & Security, GE – Principal Engineer

I think they got too specific here and they should spend less—

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I don't think that's a Privacy and Security work issue, but I think the big problem is there isn't—I'm not aware of a widely deployed standard for handling amendments.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

This is it.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think the Tiger Team is going to run into that. They're going to want more, and there isn't a good standard to rely on.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I think whenever you talk about embedding an electronic link into something, that is a security issue.

John Moehrke – Interoperability & Security, GE – Principal Engineer

That's why I've targeted as to what authority is that linked. How do you know that it isn't changing day to day?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Exactly. How do you know it doesn't become dangerous? You don't know. Whenever you embed a link, you're introducing risks.

John Moehrke – Interoperability & Security, GE – Principal Engineer

Which, I know, David, you and I have had some offline discussions about that. Again, I think they said probably more than they need to here. Is there really a problem with EHRs not having an amendment functionality and is just simply saying they need to have an amendment functionality demonstrated sufficient?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, maybe we should say it started with over specified.

John Moehrke – Interoperability & Security, GE – Principal Engineer

These are all good preamble comments.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Okay.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

The one that I didn't get quite well was number 11, enable user to electronically obtain their response. So, of course, this is sort of like the provider writes a letter consistent with HIPAA privacy that says I received your request to amend, but I am not abiding it because I, whatever. So, this is saying that the EHR should have the ability to obtain a PDF of that letter into the record, or what is this attempting to do?

John Moehrke – Interoperability & Security, GE – Principal Engineer

So, usually a PDF is generically called a scanned image, but that's a good question.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think that's what the scan was referring to is an electronic facsimile of the original document.

John Moehrke – Interoperability & Security, GE – Principal Engineer

Yes, and it's better to say scanned in regulation than it is to say Adobe PDF.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

So, Walter, did you want to say anything about that?

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

Well, I have to say this is creating a bit of confusion about whether this is going down the path of now I have to electronically append or attach to the EHR record a copy of the letter maybe or the communication that I send to the patient saying I received your request to amend, but I'm not

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

I think in particular, John, right after the previous one where they were so specific about what they meant by append, then, the next one says electronically append, that we're creating confusion. Does this also mean it can be an electronic link, text or scan? I think John's comment about the previous where they're too specific makes this one even more confusing.

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Maybe it should just be incorporate instead of append so that it's less confusing.

John Moehrke – Interoperability & Security. GE – Principal Engineer

I think you will always see it as an amendment.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

That's not an appendment though.

John Moehrke – Interoperability & Security. GE – Principal Engineer

I think there are cases when you need both. There are some cases where you do a strike through like mechanism in a database-controlled sense. Then, another case where you actually add something on the end as legally required notice but it's not changing the original material. I think that's what they're trying to get at is the distinction between keeping track of it as required by HIPAA versus—

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Well, append, to me, doesn't mean strike through. That means tag it onto the end.

John Moehrke – Interoperability & Security. GE – Principal Engineer

I agree. That's why I think that's different than amend. Amend is a strike through.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

I agree.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

No. Amend is—well, boy. We're having troubles with it, but usually patient-supplied information is not incorporated into the EHR. It is appended and to incorporate it is very different.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

I agree.

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

It's almost like B there should not fall under I, which is amend because appending is not amending.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

I and II are both amending. They're both under amendments.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

That's true, but I is specifically saying enable a user to electronically amend. Then, B says obtained, as if it was an amendment to the record. The point I think to be made is that that append is not really an amendment.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes, but I think the amendment is the—that came out of the law. Didn't that come out of high-tech or something?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, I think it's coming out of high tech, but we need both amending and appending and the question is this isn't worded correctly. It says append twice.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

To organize it, I would say I should be enable a user to electronically amend and then A is right, replace existing information and to strike out and redline and all that can be done. Then, the II should be enable user to electronically append, and then, when we have a B now should be under that new II and what we have currently under II should be a new B under new I.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think it's redundant and therefore going to create trouble.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

So, the B is appending what the patient gives you. II is appending the provider's response to B.

John Moehrke – Interoperability & Security, GE – Principal Engineer

I see what you're saying.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

Exactly. That's why they should fall under the same II.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I see what you're saying.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I got you, and that's specifically called out in HIPAA, that there's kind of just three way original, the patient's response and the provider's response to the patient response are all called out in HIPAA as I recall.

John Moehrke – Interoperability & Security, GE – Principal Engineer

As needing to be recorded in the EHR?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes. Well, in HIPAA, it's not EHR, but it's recorded in the record.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

So, my suggestion, again, would be to suggest to create two Is. The first I would be enable the one that is right now and under that, the current A, and then, a new II that says enable a user to electronically append to a patient's health record. Then B, patient-supplied information, which would be a the IA, and then, what we have as II now a response to the patient-supplied information.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I think it's fine the way it is except for the point of the electronic link.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

We're not going to comment on their request for scan versus—

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Yes, we requested public comment on whether—

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Free text and scanned.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Be required to be capable of appending patient-supplied information in both free text and scanned format. That's why the Tiger Team was talking about that. That's right. We wanted these messages to be certified. That's why we've talked about that. Now, it rings a bell.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I would argue that's not a Privacy and Security issue. That's an operations

John Moehrke – Interoperability & Security. GE – Principal Engineer

You Tigers can argue that one.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Okay.

John Moehrke – Interoperability & Security. GE – Principal Engineer

What about a patient supplying a consolidated CDA form? Is the patient allowed to supply those?

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Yes, as long as you can append them.

John Moehrke – Interoperability & Security. GE – Principal Engineer

Well, because they're not free text and they're not scanned.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

If they do supply a consolidated CDA, you probably have a diagnosis already. Just kidding.

John Moehrke – Interoperability & Security. GE – Principal Engineer

We don't have the diagnosis yet.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

That's an interesting point because in the future if a patient points to their PHR and—

John Moehrke – Interoperability & Security. GE – Principal Engineer

I want to amend my EHR with this CDA.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Yes, that could be electronic. It might not be free text or scanned.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

My bet is that when they said free text, they just meant text. They didn't mean free text in the sense that we mean it as in unstructured text.

John Moehrke – Interoperability & Security. GE – Principal Engineer

I think they did.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

I think that's what they were thinking, but it could be structured if it's coming from a PHR.

John Moehrke – Interoperability & Security, GE – Principal Engineer

Agreed. It could be structured if it's coming from the patient.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

John Moehrke – Interoperability & Security, GE – Principal Engineer

I can send you my consolidated CDA from a health ... if you want.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes. So, you said—

John Moehrke – Interoperability & Security, GE – Principal Engineer

I can even send you some DICOM images.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes or DICOM images. So, John, you said they are too specific. What would you suggest—how would you suggest they change that B to make it less specific, append patient-supplied information?

John Moehrke – Interoperability & Security, GE – Principal Engineer

Yes, I think what they're trying to get at it is setting some minimal bar to say that the EHR technology has to at least be able to handle X as a minimal bar for patient-supplied amendments. If that minimal bar is—it should be actually worded as if it's a minimal bar. A minimal bar of free text would be fine. That then allows you to go above and beyond by supporting CDA. Then, I would just put a period. Stop.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Don't you think, John, that maybe the question they're asking when they solicit comment is whether that minimal bar should include support of scannable material knowing that that's perhaps an incremental complexity, a significant incremental complexity for some vendors?

John Moehrke – Interoperability & Security, GE – Principal Engineer

Yes. I think the problem though is you get into well was it scanned by the patient or was it scanned by your medical records department and attached, and I think that I don't mind that, but I think it should be phrased as a minimal, to minimally accept free text or scans and the scanned. I guess maybe that's our question is are there any ... or—

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Is the scan part of the minimum, I think is the question. I think the answer probably has to be yes it is given that there will be relevant material that's not admissible with anything other than a scan and even though it does introduce some complexity to vendors, but I also don't think it's a privacy question or a security question. I think it's an operations.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Operations. So, do you think that we should—what I have recorded is that it's over specified. B is over specified. Do we want to say it would be better to say append patient-supplied information?

M

Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Okay.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, somebody will have to write a certification test for it so they'll come back to somebody and want to know what does that mean, but that's not our group.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Okay.

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

Can you append a structured document? I suppose you can amend it.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And you have to scan it first.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Well, you still want to append it. You wouldn't want to just replace it as if it were from another provider or something. You'd never replace it. Automatic log off, we have several more here. Automatic log off—terminate—now, this is one where we tried to make a distinction between a session lock and a termination. So, we said that it should be able to initiate a session lock and then how to get it back after that and must be able to terminate an electronic session and then a systems administrator must be able to set the time period. They just put terminate an electronic session after a predetermined time of inactivity and didn't put any of those—didn't put session lock or the ability to set things.

John Moehrke – Interoperability & Security. GE – Principal Engineer

This is a classic one that's very difficult to specify. On the other hand, if it's really a problem, is there EHR technology out there that has not already figured out how to do this for daily workflows?

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

That's basically what they're saying is yes, you can still do the session lock if you want to, but the real test is the EHR technology able to terminate a session including terminating the network connection.

John Moehrke – Interoperability & Security. GE – Principal Engineer

But see, terminate is a problem because what if I'm in the middle of editing?

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

But that's not inactivity.

John Moehrke – Interoperability & Security. GE – Principal Engineer

I was called away. I was in the middle of editing. I was called away. The system is supposed to terminate. What is it supposed to do with the partial edits that I've made? It can't commit them. So, now you're forcing everybody to add some technology by which it can save the edits. What if I'm using browser technology? Now, you're forcing me to move this technology to the client side. I can't use

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Well, I think what they're saying is they're not forcing you not to provide—they're not precluding you from providing other options.

John Moehrke – Interoperability & Security. GE – Principal Engineer

No, but they're forcing me to be able to terminate always.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

To be able to, that doesn't mean that you always did that, but you should be able to.

John Moehrke – Interoperability & Security. GE – Principal Engineer

I know, but If I am forced to terminate in all circumstances, I have to write a lot of client-side code, just purely to pass the test.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

You're right.

John Moehrke – Interoperability & Security. GE – Principal Engineer

I personally think this whole line item is dated and doesn't even need to be in certification criteria. ... EHR technology today that doesn't have conceptually the meaning behind what we're trying to do as in please, if the system is inactive, don't continue to show the PHI that's on the screen. That's a pretty darn common functionality and by putting it into certification criteria, again to Walter's point earlier, we're writing a standard rather than referring to one, and I just don't think it's necessary.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

I don't think that what they have written here accomplishes what is in their preamble either. They say there that the EHR technology must have the capability to terminate a session including terminating a network connection. Well, terminating an electronic session doesn't terminate a network connection nor would you want it to.

John Moehrke – Interoperability & Security. GE – Principal Engineer

Not in all cases, correct. Except client cases, no, you don't want to terminate the network. I think the time for this specification is gone. It's commonly implemented.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

So, is that we want to say, unnecessary? It's called automatic log off. I know that's HIPAA. All this is HIPAA work. Terminate an electronic session is HIPAA work, but an automatic log off doesn't terminate—it terminates that person's session, but it doesn't terminate a network connection.

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

This is almost copying the exact wording from the HIPAA security implementation specification of that implemented mechanism that terminates an electronic session after a predetermined time of inactivity. So, this is doing nothing but inserting that into the certification criteria, which as John points out, is already part of the common practice. Now, to David's point, is it important to ensure that even though it's sort of a common practice, it is included in a certification rule as a statement because this doesn't even have a standard? It's just saying terminate an electronic session.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

So, what do we want to say about this? We know it's in HIPAA. We know they have to be able to do it to pass HIPAA. Is there a better way to—what do we want to do with it?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Would it make sense to try changing the language to something like render inaccessible access to any PHI after specified period of time without using words like terminate? The point is obvious—pardon, go ahead.

John Moehrke – Interoperability & Security. GE – Principal Engineer

This is closer to the words you find in HIPAA.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

This is exactly what's in HIPAA. These are the exact words that are in HIPAA.

John Moehrke – Interoperability & Security. GE – Principal Engineer

Terminate an electronic session?

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Yes.

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

Yes.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

I have the HIPAA matrix open in front of me.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

That's exactly what it says in HIPAA. That's why it's always been in question.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

It's one of these things where we know what it means. It's just hard to put it in language.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Implement an electronic procedure that terminates an electronic session after a predetermined time of inactivity. So, that's what HIPAA says.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

It is different from EHR technology.

M

Exactly.

John Moehrke – Interoperability & Security, GE – Principal Engineer

Well, actually if you look in the NIST 800-53 that we pointed at, which actually was just revised, it goes on and on. It's not easy to explain.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

So, what do we want to recommend? That this—it is in the law.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Dixie, what does it mean here where they indicate that this is an unchanged criteria because if it's unchanged and people haven't struggled with this so far, maybe we just want to leave it alone.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

That's what it means. It did not change anything from Meaningful Use Stage One.

John Moehrke – Interoperability & Security, GE – Principal Engineer

So, that's why I didn't comment on it. I was wondering why I didn't comment about it on my blog. I'm like okay because it did not change. It's original.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

... the access the same thing.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Are we aware of any issues from Stage One that need addressing?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I think that's the task of specifying test procedures is where we're really going to get—that's when it's going to become challenging.

Walter Suarez – Kaiser Permanente – Director, Health IT Strategy

Since this is unchanged, the test procedures wouldn't change either, right?

John Moehrke – Interoperability & Security, GE – Principal Engineer

Right.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

I'm not sure they even exist. I'm trying to find any that exist, as you know. You've been copied. So, ... so we don't want to comment on?

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

I would leave it alone as David suggested.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Encryption of data at rest.

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

Emergency access, we're doing the same, leaving it alone?

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Yes, it didn't change. It says it's unchanged. That's why I just moved on. Is that true?

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

That's true. Let's keep moving.

John Moehrke – Interoperability & Security. GE – Principal Engineer

The actual text in the regulation is better than their description, by the way. The description gets into all kinds of misunderstandings of the emergency room versus ... versus a catastrophic emergency, but the actual regulation text is

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

But you have no comment on the actual text?

John Moehrke – Interoperability & Security. GE – Principal Engineer

The regulation text is fine.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Okay, let's go to encryption of data at rest. You'll recall that we based this on the secretary's guidance for a breach encryption around to avoid breach notification. We said general encryption EHM is being able to encrypt and decrypt in accordance with the NIST algorithms. Data at rest, we said technology who's functionality includes the capability to manage electronic PHI and the end user device storage, must be able to encrypt and decrypt data persisted on those end user devices. We referred to 140-2 NXA and also the NIST.

So, what they said is similar to that but with a little bit more detail. If EHR technology manages electronic health information on the end user device and the information remains stored on the device after use of the EHR technology on that device has stopped, the electronic health information must be encrypted in accordance with This capability must be enabled by default and must only be permitted to be disabled by a limited set of identifying users. Then they said information managed by EHR technology never remains stored on end user devices after the use of the EHR technology on those devices has stopped. So, comments?

John Moehrke – Interoperability & Security. GE – Principal Engineer

You probably want to do the same thing with the limited set of identified users with a set of authorized users so as not to say there is some limit.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Yes, that's something that technology can actually do. Good.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

A different point, I agree with that one, a different point, in one of the groups that was discussing this, the question came up about potential retention of data in operating system controlled resources like swap

files or paging files, and particularly I think under IOS and Android, there may be some things that are inaccessible to the average developer but would conceivably under a hacker attack reveal cached data. I don't know if we just don't specify that, or do we specifically want to address operating system protected resources that are outside the scope of application control like paging and swap files.

M

I would stay away from that.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

I would too. First of all, there's no such thing in accessible data.

John Moehrke – Interoperability & Security. GE – Principal Engineer

Well, the alternative is to require that the device encrypt everything, but that would rule out some very important mobile platforms.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

But if you use a device and it stores something in storage and deletes the file, the image of the deleted information remains on the disk, right?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

No.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

You don't want that to remain on the disk, right?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

So, do we think that it should require encryption? Well, it does require encryption for the part that the application controls but there may be copies of that data persisted elsewhere that you can't change with just your applications control, like swap files.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Yes.

John Moehrke – Interoperability & Security. GE – Principal Engineer

Yes, but I think you're getting into again, such wordsmithing in a regulation that is specific to current technologies and really it's out of the control of the EHR technology in that case. What we wanted them to do was encourage EHR technology that never saves actively the PHI on the device, and they've done that.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

They did just what we recommended, and actually, I think they did it better than we did, quite frankly. It is 8:00, well 11:00 you guys time. We have how many more? Integrity and accounting of disclosures and that's it. Do you guys wanted to—well, accounting for disclosures, well, that's an unchanged. Accounting of disclosures has not changed. Integrity is—

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

This is pointed at the ...

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

It's pointed at So, do we have anything we want to—

John Moehrke – Interoperability & Security. GE – Principal Engineer

The only thing we—I'm not sure whether it under integrity is really necessary. Effectively, they're forcing you to verify and if it's part of a transport as in Direct Project or COS, even COS applies to anything, it's automatic, so, it's not a problem. But what if it comes in as a digital signature? Are you forced to validate every digital signature? ... but it may not be necessary.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I got dropped for some reason. I'm sorry. I didn't mean to cut off in mid sentence.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Yes, I know. It's end of our time, but I thought we had just one more.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

What are we talking about now?

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Well, the technology does need to be able to verify it or else you may as well not use it to begin with.

John Moehrke – Interoperability & Security. GE – Principal Engineer

Be able to verify, sure. ... verify—

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Be able because this is certification criteria, has to be able to verify.

John Moehrke – Interoperability & Security. GE – Principal Engineer

Right, but it could be able to verify upon a user request to verify.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Right, but for certification, it just has to show it can—

John Moehrke – Interoperability & Security. GE – Principal Engineer

Well, we can deal with that when we look at the certification scripts.

John Moehrke – Interoperability & Security. GE – Principal Engineer

It was a super minor ..., so I'm fine with it.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Yes, the test procedures are going to be much more challenging, I think. So, I'm glad we had help doing those.

John Moehrke – Interoperability & Security. GE – Principal Engineer

I'll put ... that both under the encryption address and the integrity, those are also places where a proper key management is important. So, there are plenty of references to 210-A and 210-C that really should be making sure that key management is done properly too.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Key management is not a—well, EHR technology has to be able to manage Yes, that's a good point. So, do we want it to get the key management?

John Moehrke – Interoperability & Security. GE – Principal Engineer

We need to very carefully figure out how to specify that because this gets back into the discussion we were having before about wait, over specifying X509 is going too far, but under specifying key management is also troubling. Since there are places that refer to the hashing and the encryption algorithms, it really should be referring to hashing and encryption and team management. All three of those would just be the fifth specification. So, again, we're pointing out but we're saying it's key management hashing and encryption.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Okay, I got it. Thank you for sticking around for those three extra minutes. Can we open this to any public comment just quickly?

Mary Jo Deering – ONC – Senior Policy Advisor

Please, operator, would you open the line for public comment?

Coordinator

We have no comments at this time.

Mary Jo Deering – ONC – Senior Policy Advisor

Dixie, you do have another call next week for two hours on the 29th, 2 to 4 p.m.

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Alright. Thank you for that reminder, and—

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

So, what we'll do is wrap up the notes and send them to the group and maybe the first part of the next call, we can just finalize the recommendations. Is that the plan, Dixie?

Dixie Baker – Science Applications Intl. Corp. – CTO. Health & Life Sciences

Well, I think we can finalize—they're not really—unless there's some—we'll write up the comments. Walter and I will get together and distribute them for your review and if there are—if we failed to capture any of your comments, then we'll discuss those at the next meeting, but it seems to me our next meeting, we should be able to start on the test procedures discussion. Thank you all for calling in and for your participation. We really appreciate it. Have a good day.

John Moehrke – Interoperability & Security. GE – Principal Engineer

Thanks, Dixie.

Walter Suarez – Kaiser Permanente – Director. Health IT Strategy

Bye.