

**Privacy & Security Tiger Team
Draft Transcript
August 6, 2012**

Presentation

Mary Jo Deering – Office of the National Coordinator – Senior Policy Advisor

Good afternoon. This is Mary Jo Deering in the Office of the National Coordinator for Health IT. This is a meeting of the Health IT Policy Committee's Privacy and Security Tiger Team. It is a public meeting and there will be an opportunity for public comment at the end. And I would ask the members to um give their names when they're talking; thank you very much in advance. And I'll begin by taking the roll. Deven McGraw?

Deven McGraw – Center for Democracy & Technology – Director

Here.

Mary Jo Deering – Office of the National Coordinator – Senior Policy Advisor

Paul Egerman? Dixie Baker?

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

I'm here.

Mary Jo Deering – Office of the National Coordinator – Senior Policy Advisor

Dan Callahan? Neil Calman? Judy Faulkner?

Judy Faulkner – Epic Systems – Founder

Here.

Mary Jo Deering – Office of the National Coordinator – Senior Policy Advisor

Leslie Francis?

Leslie Francis – National Committee on Vital and Health Statistics

Here.

Mary Jo Deering – Office of the National Coordinator – Senior Policy Advisor

Gayle Harrell? John Houston?

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Here.

Mary Jo Deering – Office of the National Coordinator – Senior Policy Advisor

David McCallie?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Here.

Mary Jo Deering – Office of the National Coordinator – Senior Policy Advisor

Wes Rishel? Micky Tripathi? Latanya Sweeney? Are there staff on the phone who would like to identify themselves, please?

Kathryn Marchesini – Office of the National Coordinator

Kathryn Marchesini, ONC.

Mary Jo Deering – Office of the National Coordinator – Senior Policy Advisor

Anyone else? Okay, back to you, Deven.

Deven McGraw – Center for Democracy & Technology – Director

All right, great. Thank you very much, Mary Jo. What we are going to do today is to report on the results of the Health IT Policy Committee meeting of August 1, so just under a week ago, where I presented our initial recommendations on identity and authentication of provider users of EHR data. And we got a request from the Policy Committee for some additional work on the scenarios for level of assurance three as a baseline, and that's essentially what we want to spend our time doing today. So we have this call today, we have another call um on August 20th um and then we're aiming at the Health IT Policy Committee um meeting which will take place on Wednesday, September 6th.

So generally what happened in the Health IT Policy Committee meeting, and a number of folks on the who are on the call today were actually also at that meeting, so um I'll count on them to chime in if I'm missing anything or misrepresenting anything, but generally there was agreement um by the Policy Committee that um that we ought to have a baseline of level of assurance three per the NIST standards for riskier exchange transactions. There were some questions that came up about you know sort of what the, what are those risky transactions and in, and in particular there were some folks who asked about cloud computing. We really didn't dive into that in too much detail.

More questions were raised about what the time burden is on physicians and other users of EHRs, you know, focusing on a, largely on use cases for access to information within a facility or within a practice um, which is a a kind of scenario that we had to initially identified as not necessarily being one where we would call for a you know a specific baseline standard to be set. Um, but nevertheless, it just underscored the need to sort of drill down with a little bit more specificity on where we think these riskier exchange transactions exist and what are the criteria that make them risky which might help us, or help ONC in the future determine when something sort of triggers the need for you know a level of assurance that's greater than the one that's typically used today, which um is largely user name and password at level of assurance two.

I'll pause for a minute and see if anybody who was who was at the meeting wants to add anything or even folks who were not at the meeting and have questions. I mean the general gist is that conceptually the committee was with us but they wanted to see us do a little more work on the use cases or the scenarios um where we thought that a baseline level of assurance three would be warranted.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Deven, this is David McCallie with a question.

Deven McGraw – Center for Democracy & Technology – Director

Sure.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I assume that if the assumption is that occasionally there's a need for level of assurance three, that means that all identity proofing, which is presumably just done once, would have to be done at level of assurance three. Is that, was that discussed?

Deven McGraw – Center for Democracy & Technology – Director

It was discussed a bit. The general, the committee members liked the idea of a phase in to full level three um with the sort of 2.5 scenario where you don't necessarily have to meet the fullness standards on the identity proofing side for level three for an interim step, but that ultimately when we thought you know that ultimately, but that was more of a sort of timing issue, how you phase up to level three versus whether you would require, say, 2.5, as we've come to call it, for some exchange scenarios and full on three um for others, and of course we know in the case of controlled substances that it's really level of assurance three plus, because it's much more specific about what's required on the authentication side. But I think, you know, it's open for us if we're sort of, if there's a particular set of exchange transactions where we want to see the greater assurance on the authentication side, but maybe less concerned about identify proofing per NIST standards, you know, that's something to think about. You know another topic that we might also um think about is one that was raised during public comment, which is that which is the use of biometrics as a way to um to authenticate um as one of the tokens, which is not actually currently part of the NIST um 800-63-1 framework, as we know.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, so, this is David again, where I was headed is that if the assumption is that we would have some kind of a phased ramp up of the proofing um criteria to eventually land at level three, then the question you originally proposed is really about what are the use cases for two factor authentication as opposed to single factor authentication, and what qualifies as an acceptable second factor.

Deven McGraw – Center for Democracy & Technology – Director

That's, I think that's a, that's a fair way to put it.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Because you can't, if you're identify proofed at less than level three, you can't ever be level three unless we are all comfortable that being identify-proofed at this 2.5 plus two factor authentication is what we mean when we say level three authentic assurance.

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I'm just trying to decouple the two, because proofing just happens once –

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

... whereas the decision to use one factor today and two factors tomorrow could vary, you know, reasonably by the circumstance.

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Okay. I –

Deven McGraw – Center for Democracy & Technology – Director

That's a, that's a fair point, David. That makes sense to me.

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

Yes, that's a great point. This is Dixie. I have another question.

Deven McGraw – Center for Democracy & Technology – Director

Sure.

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

Did they discuss – did they make a distinction between authenticating an organization versus, or a server versus authenticating a person?

Deven McGraw – Center for Democracy & Technology – Director

No, because we said at the outset um that we agreed that the digital, you know that our recommendation on digital certificates would we still thought it was acceptable to have those issued in an organizational level. The conversation we were having with the Policy Committee is whether we required those organizations to be authenticating or credentialing their individual users at a certain level and in what circumstances would they do that. So we really, we focused on that specific question, when would we require organizations to credential individual users at baseline LOA three, in what circumstances.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Thanks. This is Wes. I joined late. I just wanted to ask another question. Um, in in in the case of accrediting users is the scope of that accrediting users for health information exchange or accrediting users for using systems that have protected health information even though they're just used within the enterprise?

Deven McGraw – Center for Democracy & Technology – Director

I'm not sure that precisely answers your question, Wes, but we started with the assumption that we're talking about a set of policies that would apply to exchange transactions for meaningful use in terms of the purpose for which information is being exchanged. But –

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Okay, well I think that's helpful. I agree it's not, if it's not solid clear it's certainly clearer than I was a minute and a half ago.

Deven McGraw – Center for Democracy & Technology – Director

Okay, thanks.

Judy Faulkner – Epic Systems – Founder

Deven, I'm not quite sure about your, if I understood your answer. In other words, if I'm just using, if I'm in a position just using the software, not doing an exchange at all with any organization outside of my own, is that covered or not covered by what you just said?

Deven McGraw – Center for Democracy & Technology – Director

Oh, you know, good point, Judy. I, honestly I think that we may have played around the boundaries a little bit, if not grossly so, in our exchange scenarios. We've always tried um, or historically have tried, with our recommendations to try to aim them at um data exchange, on the theory that um that that's sort of where the sweet spot is for thinking about additional policies around privacy and security, right? And so, hence, we sort of set the, set the framework and set our universe for the Policy Committee as saying that we were talking about exchange of data um for purposes of meeting you know the meaningful use criteria, which narrows even further the universe that we're really aiming at here. On the other hand, I'm looking at the exchange scenarios that we put before the Policy Committee on the slide and thinking about the discussion that we had at the Policy Committee the very first um scenario that's up there is essentially internal access to your own system, which one could argue is not exchange really at all um depending on how you think about whether the access by medical staff to an institution's system is or isn't you know an exchange or a disclosure, but we really are not necessarily being clear about where our boundaries are. I think it's really our choice when we define what are the transactions where we think it's justifiable, necessary trust building, trust enhancing for us to say to organizations you should be credentialing your users who have access to PHI at beyond level two for these types of transactions. I think we can, I think it really is incumbent on us and the Policy Committee ... to draw what those boundaries are, because I think we've kind of not always been entirely true to them even in even in our own thinking about this.

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

You know I think, and I know this is sort of, I don't think we've ever addressed this directly, but um but there's it's almost like two dimensions, it's like where does the risk level reach a point where you want, you, where authenticating an organization is insufficient and you want to actually authenticate the individual, like, like controlled substances. I don't think, you know, you would want, there are there are certain points in the risk, you know, in the risk profile where you go you know I want the individual authenticated, and then on top of that as sort of another, you know, um orthogonal to that, at what point do you want that individual authenticated at level three. You know, I think at, there are some transactions where you might want a higher level of assurance of an organization versus at what point you really, you know an organization isn't enough, and I want to know exactly who that person is.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

Okay, can I – this is John Houston. Can I suggest there is another dimension to this as well, to what Dixie just said? And I think there's also this this aspect of the burden to the provider or the burden to the actual staff or individual in terms of the use of that particular level of assurance so that and what the argument is that the burdens for internal use may be so high and that it's going to push us down a little bit, whereas, if the burdens are less because of allowing the transactions when they're going external from an organization may allow us to give a higher level of assurance because the burdens just aren't that great.

Deven McGraw – Center for Democracy & Technology – Director

Right. Well, I certainly think, you know when I was trying to piece through myself about why intrinsically even as a privacy and security advocate, I get more comfortable with the idea that for you know internal access you know we, it might not be justified or it may be premature to suggest we'd have a require organizations to credential people at or at least authenticate people um with two factors. Part of it is you know that there are other indicia of security that that might help to mitigate some of the risks, but burden is another one and what's the impact on patient care.

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

Yes, yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And this is David. I, I'll throw yet another you know issue that complicates the decision making here, which is we're not yet talking about a single identity that you can proffer to a variety of relying parties um, I mean that's the NSTIC future –

Deven McGraw – Center for Democracy & Technology – Director

Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And in a few places the single sign-on, maybe that's getting closer to reality, but I suspect in the majority of places today those providers have actually multiple credentials issued by the relying parties directly, so the local HIE may have issued their own log-in and password and other associated factors, if they choose to do it that way, independent of what the provider has when he's practicing in his hospital and his EHR, which may yet be independent still from yet another healthcare resource that he might have access to, like maybe his direct HISP account, just to pick something out of the blue.

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

So it's, you know we, we loved a world where you have one credential that can be applied in all those circumstances but I don't think we're going to be there widespread for quite a while. So we have to decide you know for each issuing entity, I mean so an HIE might say the only thing we accept is two factor authentication and we require direct log-in even if you're coming in through an EHR, in another community they might say, well, we trust the EHRs in our community to proxy appropriate identities and we won't demand a second log-in.

M

Agreed.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Judy Faulkner – Epic Systems – Founder

And it's often not the physician who's going to log-in, it might be someone administratively who is logging in to get that data from a third party and then making it available to a variety of physicians who are treating that patient.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes.

Deven McGraw – Center for Democracy & Technology – Director

Well, right, but then you know, again, we would expect that person to have, to be credentialed in some way.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes.

Judy Faulkner – Epic Systems – Founder

Right. And so the physicians seeing that data aren't necessarily credentialed at level three, but the person who's getting the information would have the higher requirements –

Deven McGraw – Center for Democracy & Technology – Director

Right.

Judy Faulkner – Epic Systems – Founder

... only.

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

Um, yes.

Deven McGraw – Center for Democracy & Technology – Director

Well, that's right, but keeping in mind that the, you know, that we're not trying to solve the access issue just through the win—through the lens of credentialing. We're trying to solve trusted credentialing and needing to know that that that staff person who is seeking that data is who they say they are is the you know in order to create assurance around that transaction is what we're trying to solve for.

Judy Faulkner – Epic Systems – Founder

But are we trusting the organization to make sure that the person who is sitting there at that desk in the in the office bringing data over is the right person, because already you've authenticated the organization.

Deven McGraw – Center for Democracy & Technology – Director

Well, that's right, and so just to take us back to where we were, I think more than a year ago we said that you know certainly for identity proofing and authenticating users within your own system we didn't necessarily need you know to set a requirement for people to do beyond what would, what would put them at a level of assurance too. Certainly organizations could go beyond that and we're getting increasing evidence that that some are, um but we said even back then for remote transactions across an in- unsecure network, there ought to be a, that something beyond level of assurance too was needed and we were reluctant to go all the way up to level of assurance three at that time because we didn't like the paucity, the lack of good options for the second authentic – for the second token on the authentication side um that was available at that time under the NIST framework. So in many respects this sort of second bite at the apple is about deciding what we meant by remote and whether we're now comfortable with the additional options, many of them reliant on mobile technology um to do that second authentication factor, and again the sort of exchanges of data across the network, um particularly in circumstances where it may not be secure.

Judy Faulkner – Epic Systems – Founder

I agree with you on the remote and the handheld.

Deven McGraw – Center for Democracy & Technology – Director

Well, that's essentially what we're trying to get at here.

Judy Faulkner – Epic Systems – Founder

Yes, I'm still not convinced though if the person's sitting at a desk or an authorized workstation that that person should also have to do third level authentication, because in reality it's going to be a huge amount of the organization that has to have that um ability because lots of different people could be in the surgery that they decide to get it, it could be all different places that they decide to get that information. It doesn't have to be just in, just that they register, for example.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

If, if we could – listen, let me take another stab at my original question now.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

We um, as I understand it there are two drivers leading us to this discussion. One is improvements in technology for multi-factor authentication. And the other is concerns about governance with health information exchange, particularly, well just health information exchange.

Deven McGraw – Center for Democracy & Technology – Director

Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Um, and the issue on governance of health information exchange has been, and David will correct me if I get the buzz words wrong, transitive trust, do I trust, as a health information do I trust organizations or do I trust people. And the vast majority of all solutions have been I trust my HIE to trust every organization in the HIE so that I don't need to trust my HIE to know about every person using every system that might be connected to the HIE. That's the steady state right now. Um, if we were to say we'd like to reopen that issue based on the changes in technology I think it's important to recognize how big a change we would be requiring industry to undergo in order to take advantage of the new technology, um, if in fact just the idea that that 5 hospitals and 2,000 practices in an HIE would coordinate ... or use an external, the same external resource to identify the 10,000 users for hospital and 10 users per practice is quite an ambitious undertaking.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Going, moving from current authentication technologies, which can be rated in terms of the number of factors but are sourced from many different sources, to one that uses only those factors that are administered through this common administration, it's another, it's another change that would take years and years to accommodate in the organizations that are members of health information exchange. Um, so I think the issue that Judy raises is an issue of, of ... importance to us, um, and we have to be careful to not fall into the common technology trap of seeing that because there's an easier technology, that all of the administration and workflow processes around using that technology are also easy.

Deven McGraw – Center for Democracy & Technology – Director

Right, right. So I think that that, I think that's a really good point, Wes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

On the other hand, you know, Wes' point is completely valid, it's non-trivial work, on the other hand, you know the lines have been drawn in the sand, certainly with the DEA, that says too bad, you're going to have to do that work, meaning manage things at the individual level where individual non-repudiation is, is demanded um, I can prove that you signed this prescription, doctor. And the , you know ongoing work, for example, at EMSD, the electronic submission of documents to CMS is headed in that same direction, it's not finished, but it's going to land there almost for sure, of individual assertions of identity um and –

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Let me ask a question. In those two cases are those assertions of identity through a common administered factor?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Um, no, they're individually signable, you know think –

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

As I understand, and I could, I have to look at it closely, but as I understand describing controlled substances, it's adequate for each site that uses ePrescribing for controlled substances to establish their own source of certificates for individuals, and that they, they stand to demonstrate a trust chain back to some, some authorized user. But that's a lot less centralized and bureaucratic than saying they all have to use the same common source. And common could be as broad as all of the federally um affiliated issues of certificates, but it's just a lot, a lot more complex to administer, if I understand it correctly.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, and I can't comment exactly on that, Wes. Um, the thing, I think at worst it's certainly not a single source, it's a single source that follows an acceptable policy such as the federal bridge policy, so they would be multiple sources, they would just all follow the same policy. Whether an individual –

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

They're all, all certified as following the same policy?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Correct, correct. They would be members of the federal bridge or approved issuers of identity as per the other federal, FICAM, I guess it is.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Okay, and that –

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And that was really just to say that individual identities are coming and they're going to come, not through this committee's work, but through these related federally driven efforts around electronic submission of documents and EEA.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

So the wor – we have someone that does, that can do the staff work and it would be worth knowing whether, what are the conditions for individual identity under the DEA regulation. Is it, is it enough for the organization to issue their own certificates, or do they have to be issued from a ... that is certified as being associated with the federal bridge.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I can –

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Or, can the organization be certified to grant certificates through some certification process for them?

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I can certainly get that answer. I just don't have it right in front of me. I've read it. I just don't recall exact details. But –

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

I thought that was still evolving.

Deven McGraw – Center for Democracy & Technology – Director

Yes, I'm not sure for the DEA, but we certainly did get um testimony at our hearing that would, you know, enable organizations to still do the work of credentialing um, such as for government access, right? But they might have to attest that they've actually, for their individual users, ID proofed them –

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I think that's a pivotal, pivotal point in our discussions, whether individual identity vetting extends beyond the organization that that is issuing the credentials for access to their system, where the system collected HIE. Because, you know all hospitals have rather thorough credentialing capabilities for their staff and particularly their clinical staff, um and this fits well into their workflows, if they don't have to change the source of their credentials or the mechanisms by which they're verified or things like that. And I have to admit I'm a little vague on how these new second factors interact with digital certificates. I thought a lot of them were sort of certificate free.

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

They can be. But that was that, I would agree that at our hearing we certainly got (clears throat) we got many people who testified who said yes, I trust the organization to um identity proof their individual people. Unfortunately, we didn't get testimony at all from DEA um so it seems like what we're seeing is that the industry certainly prefers that to use the processes that are currently in place, but we don't have an official you know, an official declaration from DEA at this point. That, that's just my opinion.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

I get the sense the DEA doesn't really want to telegraph their position.

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

Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Well, they're pretty close to implementation, though. I mean, at some point you have to, if you want people to implement you have to telegraph a certain amount, right?

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

Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I've got ... and I've got some of the DEA stuff in front of me here um –

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Let me rephrase that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

... answer all the questions, but for individual practitioners working outside of an organization, in other words practice, solo practice kind of settings, you have to get your identity proofing through an authorized third party, a credential service provider, or certificate authority, at NIST level three and there's rules about how to do it in person with a government ID, or remote with a government ID and a financial account number being verified. And then institutional providers are able to follow those rules, but to do it themselves. It doesn't have to be through a third party CST.

Deven McGraw – Center for Democracy & Technology – Director

Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

So they can do it themselves. And what I'm not clear on is the tokens for non-repudiation, who's issuing those, and I'll have to just go and do some research on that.

Deven McGraw – Center for Democracy & Technology – Director

Thank you, David.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Can I suggest my –

Deven McGraw – Center for Democracy & Technology – Director

Yes, go ahead, John.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

My comment was more related to the fact that I don't think, I don't think ... the DEA feels as though um it needs to worry about engaging us in this conversation. That's my own, that was my earlier point. I understand they're close to putting things out, but you know they're going to do what they want to do –

Deven McGraw – Center for Democracy & Technology – Director

They're going to do what they're going to do, that's right. But I actually think the information that David just conveyed is very helpful to us because we, I think, have always presumed that many exchange transactions will take place with a, from organization to organization in terms of the machine to machine handoff using an organizational digital certificate. I think the question that we're diving into is whether for in order to achieve that transitive trust that Wes referred to earlier, and I thought you used the right term but I'm sure someone will correct both me and you, Wes, if we're wrong, that there might be a certain set of riskier transactions for which we would ask organizations to meet a minimum threshold with respect to their own individual credentialing. And if that's level of assurance three, what set of transactions are we talking about. Certainly the –

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

And for their own organizational credentials.

Deven McGraw – Center for Democracy & Technology – Director

Well, I don't know how an organization uses a second factor, and we didn't really go there. I mean I, this has really been about individual level credentials and whether there are a set of transactions for which we would ask people to meet a minimum standard, organizations to meet a minimum standard, which today we do not.

Leslie Francis – National Committee on Vital and Health Statistics

This is Leslie Francis. There really are two different ... different kind of families of answers to that question as I understood it when you sent the email around. One is are there, say, types of information so um substance abuse, for example, that requires special protection and so somebody might want to argue heightened credentials um when that kind of information is being accessed. The other is, are there types of handoffs when you're accessing for this purpose or for that purpose or when you're accessing from an unknown organization to whatever, I'm just, I'm trying to think of examples, but basically there's a whole set of substance questions and a whole set of process questions.

Deven McGraw – Center for Democracy & Technology – Director

Yes, I mean we didn't, you'll see that in in the examples of the exchange scenarios in the use cases here, we did not necessarily tee up anywhere though the credentialing level would be higher due to the perceived level of sensitivity of the underlying information that's being exchanged. Um but we certainly can entertain that conversation. In general our recommendations have been to assume that all healthcare information is sensitive and to acknowledge that certain types of information are covered by special protections in the law already. But to date we have never, as a group, bifurcated our recommendations in by um making judgment calls on what is the level, you know that some health data is more sensitive than others. But I appreciate that you raised it, because it's probably a thought that that others have, that's been going through others. I mean it went through my head as well, I was just not sure um how to approach that issue um given where we had come previously and that we have sort of allowed existing law to deal with what additional hurdles are in place for data that is, that is perceived to be even more sensitive than health data generally.

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

And certainly, certainly the work that Joy's doing on segmentation is all –

Deven McGraw – Center for Democracy & Technology – Director

That's right, but we, but that's based on a recognition that already in the law there are rules that require, say, additional authorization from the patient before data can be shared and in fact when Joy updated us at the Policy Committee she made it clear that the use case that they are relying on in developing data segmentation technical standards is the sharing of substance abuse data, since that already is covered by a set of very stringent rules about when it can be disclosed and frankly, when it can be re-disclosed which makes it –

Leslie Francis – National Committee on Vital and Health Statistics

This is Leslie Francis again. I just, I wasn't raising it because I thought we needed to say those were the types of transactions, involving especially sensitive data, but because I wondered whether that was part of the motivation of the questions –

Deven McGraw – Center for Democracy & Technology – Director

Ah.

Leslie Francis – National Committee on Vital and Health Statistics

... about that.

Deven McGraw – Center for Democracy & Technology – Director

Yes, it didn't, it didn't, frankly, come up during the Policy Committee discussion. Um, it doesn't mean it won't in future discussions, but it did not.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

When you bring segmentation to the table you you'll never get away. It's so complicated. Oh my goodness.

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

With genetic, you know genetic information becoming, or easily available, it seems like that's a perfect example of something that should require a higher level of authentication.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And it has its own special laws too.

Deven McGraw – Center for Democracy & Technology – Director

Well, it does although then, you know, the segmentation, in in many states but not in all and you know that's where the issue of whether we have segmentation technology that allows you to, you know to sort of create a separate set of criteria for that data versus others um comes right to the forefront. I mean it's definitely part of the discussion. So um I wonder whether it makes sense for us to just try to define the term "remote" a little bit better since that's where we were previously in terms of sort of desiring a higher level of trust in in authentication for exchange transactions that are taking place, not within a facility but are occurring remotely across, potentially across an unsecure network, um, is that sort of a set of, at least on the question of use cases that vary based on exchange scenario, is that a place to start getting into some more detail here?

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

I, I would drop the term "remote" entirely and go with what you just said, over, if the access is over a network, some portions of which are unsecured, that's what you really care about because if it's between two buildings but the entire network is a private network, you know is that a remote – remote gets fuzzy fast and what you really care about is the potential for exposure.

Deven McGraw – Center for Democracy & Technology – Director

Right.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Right. But also, in in the context of the FDA, in the context of the DEA I'm sure the DEA doesn't care what type of connection it is. If you're dealing with a some type of a, of a prescription between the two organizations they're probably going to want to see a high, you know a higher level of assurance regardless.

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

I have a question, Deven, about your last, following on John, um that last row here.

Deven McGraw – Center for Democracy & Technology – Director

Yes.

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

The electronic prescribing, we're on the last, the function, it's just of controlled substances, right?

Deven McGraw – Center for Democracy & Technology – Director

That's absolutely right. Thank you, Dixie. Yes, yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And this is David. I can give you a brief summary of the rules around the authentication credentials for the DEA, just since we brought it up earlier, um. They allow for biometrics, unlike NIST. Um, they also allow for a knowledge factor such as a password or for a hard token. The hard token has to be ...140-2 level one compliant, it must be stored on a separate device from the computer used to access the ePrescribing application, can be done with a PDA, cell phone, smart card, USB ... or other similar device.

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

David, is that the – that sounds like, is that the final rule or is that the NPRM?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

You've got me. It's as up to date as we know things, as far as I know. I got these slides fairly recently.

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

Yes, I don't think they've come up with their final rules.

Deven McGraw – Center for Democracy & Technology – Director

It's the interim final, Dixie.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, I thought –

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

Oh, it is. Okay, good, good, good, good, good.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

It's pretty close.

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

Yes, that's very close. Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And then they have some, they have some, a lot of details around biometrics and what it takes to qualify for biometrics, which I won't go into here. But what I'm unclear of, I assume if it's a hard token with a ... 140-2 level one compliant cryptography that you're not going to get that from your local IT department. That's going to be something you get from an established credential authority, I think.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

David, can I –

David McCallie – Cerner Corporation – Vice President of Medical Informatics

... to Wes' original question.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Back to the slide for one second, too, to qualify what Dixie just said –

Deven McGraw – Center for Democracy & Technology – Director

Yes.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Um we probably need to break up that last line into two segments because I, you know you have the controlled substances and then you have the other types of substances that still need to be prescribed, but I guess aren't controlled or are ... whatever, so there still would be, isn't there still some level of LOA that still requires for those ... for those non-controlled prescribed substances, if I'm saying that correctly.

Deven McGraw – Center for Democracy & Technology – Director

So what does Surescripts require, for an example?

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Well, whatever, I mean, I just think you need to break that last line up maybe into two.

Deven McGraw – Center for Democracy & Technology – Director

Well, it is, but I don't know that we necessarily, I mean, this was what we asked ONC to prepare for us –

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Okay.

Deven McGraw – Center for Democracy & Technology – Director

... in terms of some different exchange scenarios roughly on the order of riskiness, top to bottom.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

My point, though, is that you would have – what would you say if somebody wanted to prescribe um an antibiotic –

Deven McGraw – Center for Democracy & Technology – Director

Yes, but I guess what I'm saying, John, is it's not an attempt to define every possible exchange scenario. And in fact I might argue with taking the bottom level off altogether because, as you mentioned earlier, the DEA is doing what it's doing for that set of transactions. They're not varying it based on you know whether it's a transaction that takes place securely or insecurely, it's based on you know their need to be um more aware of who's prescribing a controlled substance for diversion and other purposes and you know it's not, I just – what I'm trying to do is avoid going down the rabbit hole of you know defining an entire universe of exchange transactions that might occur under meaningful use.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

I think if we don't at least make note of ePrescribing that it's going to be questioned, and I think secondly, I do believe it's, that there is a reason to put ... second level that I described, just for completeness, because people will ask questions and I think we'd at least want to identify the fact that this is a, this is within the purview of the DEA, or at least make note of the fact that we're, or at least something we've thought about that we're not going to focus on.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, and to be, I think, boy I'll betray a little bit of uncertainty here, but I would assume that CPOE just physician order entry, would fall into your row one, EHR access via local computer terminal.

Deven McGraw – Center for Democracy & Technology – Director

Yes, well I would too. But it's the reason why, you know so CPOE what about med reconciliation, what about exchange of CCR, CCD –

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes.

Deven McGraw – Center for Democracy & Technology – Director

... CCPA. That's why I didn't want to get into the minutiae of all of the transactions that could be accomplished under the topic of the word "exchange." And, John, point well taken that if you're going to describe prescribing of controlled substances it looks weird not to have a category that says prescribing of something else. But to me our discussions have always focused on the not the purpose of the transaction or even the content of the data, but whether the transaction itself, because of how it's done, um introduces some risk that an unauthorized person might get into the mix, thereby justifying a higher level of credential so that you know that the organization has proofed the person on the other end of the transaction at a high enough level to build that trust.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

But I think, but I think part of this, though, is the dynamic and obviously why the DEA's concerned is that somebody's going to certainly be more interested in trying to prescribe a narcotic inappropriately than they are an antibiotic, so it does, it does cause there to be a different level of concern, a different level of risk, not just, you know, so I think, I think it is of value to, to at least mention it so that people understand.

Deven McGraw – Center for Democracy & Technology – Director

Okay, right, so which I get. So it's a, it's a level, an additional level of risk because of the nature of the transactions, not just the, whether the transmission itself introduces risk.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

That's correct.

Deven McGraw – Center for Democracy & Technology – Director

Yes.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

But the likelihood, the likelihood of somebody wanting to do it is higher.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Leslie Francis – National Committee on Vital and Health Statistics

Well we're saying, aren't we, is that the DEA rules, whatever they are, the ones that are going to handle that, we don't have to add additional on top of that?

Deven McGraw – Center for Democracy & Technology – Director

Oh God, yes. No, we don't have to add anything on top of that; I think is what we're saying, right?

Leslie Francis – National Committee on Vital and Health Statistics

Yes, good answer.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Right, but I think it's useful to put it on the list –

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

... as a milestone or you know mile marker because it is reality, or it will be reality for providers regardless of what else we say. So it's nice to have our stuff laid out in contrast –

Deven McGraw – Center for Democracy & Technology – Director

And compare it, right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

... in comparison to.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

So I think, I think the suggestion that your last line in the slide be modified to specifically say "electronic prescribing of controlled substances" is a good one.

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Right, we agree, it's not just any ePrescribing.

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And it's not inpatient prescribing.

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And it's DEA and we don't have anything more to say about it, for better or for worse.

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And the subject of refining your slide, I think this is self-evident but I assume that lines 1 and 2 you mean “wired access” because your line 3 specifically calls out wireless access. Are you breaking those apart?

Deven McGraw – Center for Democracy & Technology – Director

We can. Again, I don’t claim complete ownership over the chart. ONC helped us develop a sort of set of preliminary use cases, it’s our job on this call to refine them, so I think, I think that makes sense.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, because I mean I think that from a risk analysis point of view if there is a wireless link in the in the chain, you know there are new risks associated with that as opposed to a wired connection. These days I think the vast majority –

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

I think we should use the same words that we used with the Privacy and Security Workgroup ages ago, that Wes came up with. I can, I can send those, but you know it had to do with if there’s any possibility that some part of the transaction could go over an unsecured network. ...

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes ... yes exactly because I mean I was going to say the distinction between wired and wireless is you know it’s a distinction around the physical nature of the communication, but you can have a perfectly secure wireless network and you can have an insecure wired network. So it really boils down to whether it’s a secured link or not.

Deven McGraw – Center for Democracy & Technology – Director

Okay. That that sure sounds like the right articulation of where we’ve been, but let me just a devil’s advocate question, which is what is it about the security of the, of the connection that makes us more comfortable with requiring less assurance on the credentialing side?

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

Man in the middle attack spoofing, there’s all sorts of bad things that can happen when it’s an unsecured link.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, and the difference between wired and wireless, I mean there’s a physical issue there in terms of access to the, you know, to an intersection point. In a, in a wired system it’s a little harder to get into the closet where you could hijack the wires than it is in a wireless system where you can be parked in a car outside the building and snoop the signal. But in either case, if it’s an insecure link the problems will occur. So I, I think there are um you know physical proximity issues do have some role to play in the risk assessment, but the critical factor is the secure versus insecure link.

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

Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

The most critical factor.

Deven McGraw – Center for Democracy & Technology – Director

All right.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I hope I'm not, if this isn't the direction slap me down.

Deven McGraw – Center for Democracy & Technology – Director

Only if I can recognize it as one. Go ahead.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Well, you might want to slap first and figure it out later then. Um, the, why are we even thinking about communications over an unsecured link?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Right. I was wondering that question too.

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

It's a different way of defining remote. You know remote, if it's a, if it's over a private network it doesn't matter that it's remote.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Right. To me remote, remote means transaction carried on the Internet rather than on a private network.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

But, so let me, let me leverage Wes' question, Dixie, to you and say, you know, if a person, we would never condone access to health, protected health information over an unencrypted channel, would we? I mean, authentication doesn't really have much to do with it, you would never be allowed.

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

I know, but they're not, when you authenticate something you're not accessing health information, you're authenticating yourself and you have it to do whatever you have in mind to do.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, but what, my point was, say, it's going to be a meaningless statement to say you have to use level three of assurance if you're going over an unsecured, unencrypted channel, because we would say you should never go over an unencrypted channel for healthcare activities, so the level of assurance is irrelevant.

Leslie Francis – National Committee on Vital and Health Statistics

But I think, I think a mutual customers would be going over secure channels.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Right, exactly. I don't think insecure link is ever going to be allowed.

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

Yes, but when you do the authentication, that's done before you exchange the health in –

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Again, I, I want to go back to my statement. I think that the distinction we're really worried about is whether you're on the, whether you use the big, bad Internet or not, where nobody knows if you're a dog.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Um, that um there are so many more opportunities for attacks in when the full Internet is involved than when you know that the channel is secure because it's a private channel that you brought to another entity, or because it's within your perimeter that it makes reasonable sense to ask for a higher level of authentication when the Internet is involved.

Deven McGraw – Center for Democracy & Technology – Director

Yes, but going back to Wes Rishel's famous statement way back when, you know, how do you know whether the Internet is involved? You know that's –

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Don't most, don't most systems have a way of knowing whether, whether a connection is from their local network or not?

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

It could potentially go over a, yes –

David McCallie – Cerner Corporation – Vice President of Medical Informatics

You don't, it could have been upstream from that, I mean, somebody, yes, I don't know. I –

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

Yes, I don't know.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think Dixie's point, I'm going to roll the conversation back because I I'm on record as saying something that was kind of stupid, so I want to withdraw my point about –

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

And I say that all the time.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes. Dixie's right, the point is the initiation of the secure channel is what we're talking about here. So I was not thinking clearly. Sorry.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

That's correct.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Well, nonetheless, whenever I've been involved in discussions about authentication where the typical scenario is logging into a Web site rather than logging in to your company portal, okay, , um if you know the banks now do so many defensive measures that we just, we've stopped calling it in N level authentication, we just call it multi-factor or N factor, I think ... call it multi-factor because it's got you know everything involved in it from well, it's more than I, more complex than I understand anyway.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, a lot of factors, knowledge, challenge, IP validation... .

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Yes, right.

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

Is that where you're coming in from?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Yes, if you if you've used it you know that when you've come in from a computer that doesn't have a cookie store then you're going to go through you know a certain amount of hell remembering when you lived in 1947 and so forth. But –

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Or where your father lived.

Deven McGraw – Center for Democracy & Technology – Director

Or where your father lived... .

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Yes.

Deven McGraw – Center for Democracy & Technology – Director

Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

But the point is that um I agree that that the processes, the process of authentication precedes the process of communication, I would be happy to sort of separately postulate that we don't want any form of authentication where things you know are shared in the clear, except I think that is so rare that it's hardly worth mentioning anymore. Um, but nonetheless, I think the potential that we want stronger authentication where secure, you know ... secured communications are going on over the Internet versus where ... secured communications are going on your Intranet, um is recognizable and worth addressing.

Deven McGraw – Center for Democracy & Technology – Director

Yes.

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

Yes, and I think that um, at the risk of sounding stupid, no, the I think we're sort of getting two things confused here too, is that if you're authenticating yourself over an insecure link, it doesn't matter how many ... you use, right? Um, yes, I think that we need to separate the two, so we're back to, I don't know how you, I don't know to define what remote is.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Well, I'm proposing that remote means over the Internet.

Deven McGraw – Center for Democracy & Technology – Director

Over the Internet.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

... .

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

Well, I –

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, or publicly accessible networks if you don't want to just use "the Internet."

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Are there any others now? I mean –

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I don't know.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

So the question, the question that is sort of the edge case when we talk about it internally is cellular phones, I mean, in theory –

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

That's not in, Internet.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

It's not Internet, but the cost of tapping data off of, of penetrating cell phones for text messaging in a local area has gotten to be ridiculous ... like \$10,000 worth of equipment or something like that. Um, it's still not a big threat because you know you can only set it up, you have to set up a radio and you have to, you have to do it in a fairly local location, but nonetheless it's caused us to change our recommendations about the security of text messaging from what we used to get.

Deven McGraw – Center for Democracy & Technology – Director

To be stronger or not stronger?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

We no longer consider text messages to be, we consider them to, to have the same limitations as something coming unencrypted over a public network.

Deven McGraw – Center for Democracy & Technology – Director

Right.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Yes. Here's a stupid question, just as an aside. Is Internet2 still, I don't get involved in the education side, is Internet2 still around, and if so is there a possibility we would end up using Internet2 for some of this type of stuff?

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

Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Those programs tend to be grant programs, right, and when they run out of money they run out of steam.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Yes. I just haven't heard about it in a while and I just don't know what the status is and whether there are other quasi-public um vehicles that might still require –

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I would, I would argue that any of the, for any of those to become so prevalent that we could count on it in a recommendation for the near future is a pretty, pretty remote possibility.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

It's just a thought. I was just thinking of all the sort of the edge cases here.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I just have to comment on my own contributions, I was just thinking if we all got to edit out everything that we said that was stupid, just think how much, just think about how much shorter the minutes would be.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I want to come back to my point about open access networks as opposed to the, to the Internet.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Because I do have, I think one use case that's not uncommon, which is almost every hospital has a public accessible WiFi presence –

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

... inside the hospital that is not the same as the Internet.

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

Yes, that's a good example, yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

When you say it's not the same as the Internet –

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, in other words, it's WiFi that's proffered up against local area networks which is in bridges to the Internet if you hit the Accept button and agree to the terms.

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

It's peer to peer?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I don't –

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Well –

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Maybe that's another case.

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

Peer to peer is not

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Strictly speaking, we –

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

As I understand it, the effect of the WiFi is you're in a, you're in a, you're corralled completely unless you accept the terms and use and then you are not – still don't get any access as to the local network, you get access to the Internet.

Deven McGraw – Center for Democracy & Technology – Director

Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Agreed, but it's, you know like everything it's a hackable entity and I'm saying it's not the Internet access and I'm guessing if a provider wanted to access a secure resource coming through the hospital's public WiFi, we should treat that like the Internet, even though it isn't the Internet. So I think the net effect is the same. I'm just trying to be more precise when we say the Internet we mean the open access network.

Deven McGraw – Center for Democracy & Technology – Director

Right, publicly accessible open access network.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

... .

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

Which goes back to any access could go over an unsecured network.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

As long as we throw in comments such as the Internet, I'm okay.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Okay.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Or public access in a hospital.

Deven McGraw – Center for Democracy & Technology – Director

What about in an airport?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

So let me so the where we're headed toward making this distinction is that we feel like higher level of authentication might be warranted when access comes through this Internet open thing, right? Is that where we're headed?

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

Right, yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

So, so I want to ask a question and just to make sure I'm clear. Let's, let's say we have a local HIE, um, and that's the thing that we're talking about accessing and we agree that you know coming in over the Internet puts it in a riskier position, what if the physician comes to that local HIE through his hospital's connection to the HIE, are we, and that goes over the Internet, but it's system to system and maybe it even has, you know, tokens that have been mutually validated, like with Direct or with Exchange, um are we saying that in that case it's coming over the Internet but it's not the same?

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Can I suggest in that particular case it's still coming in over the Internet where you've taken, you've put mitigating controls in place which should enter into sort of a, as a, as a part of the requirement um –

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Right.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

... to maybe mitigate the need for a higher level of assurance.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

One of the factors is that you are in a system that is a trusted system.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Yes, right, a trusted link or something, yes.

Deven McGraw – Center for Democracy & Technology – Director

What does that mean?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, that's where I'm –

Deven McGraw – Center for Democracy & Technology – Director

What did you mean by that?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, that's where I'm headed, because I just think it's going to be hard to go too far on this notion of the Internet because you know mutual TLS over the Internet is pretty secure. That's a VPN basically.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And that's what exchange –

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

The same as authentication, that's securing the link. You know it's important that we keep the two distinct.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

But the –

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

You should secure the link before you pass any authentication information across it.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Right, but the point is that the securing of the link if it's mutual TLS or something like Exchange or Direct, it is token validated. It is, you've created a VPN before any traffic flows –

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

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

... even though technically it's the –

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

Right, but you still need to authenticate the person.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

But that, but that, but that then argues against my blanket condemnation of the Internet.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

That's why I raised the case. This is the challenge edge case. It says there are some uses of the Internet, like VPNs, that we would consider to be secure enough not to warrant this –

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Can I, can I –

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

VPN is not the open Internet. I thought we had – you know that’s the term that HIPAA uses “open Internet.” I think that’s the term that we’re seeking.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Can I suggest though that I think we have to be cognizant of the term “Internet” and if we’re going to make recommendations I think we have to do them in a way that people don’t have more questions than they have answers, so I think we need to recognize that a whole class of solutions will involve the Internet as being the transport vehicle. And then I think what we need to do is layer upon them one of the things that were added, such as a VPN, which provides a layer of security which will allow us maybe not to have an individual level of assurance as high as if we didn’t have a VPN in place. But I think we need to express our discussion or our solution in a way that allows people that aren’t less, aren’t as informed to understand what we’re trying to get across.

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

Yes, that goes back to our initial talk about how there are multi-dimensions here. It’s just not straightforward.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, and I think that’s what we’re wrestling with is how to express this in language that makes sense.

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

It captures all of these dimensions, you know whether you’re on a, already on a, somebody you know um a hospital’s network to begin with and you’re doing remote access, for example. It’s

David McCallie – Cerner Corporation – Vice President of Medical Informatics

It would be easier just to make it required for level three everywhere all the time, wouldn’t it?

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

Yes.

Deven McGraw – Center for Democracy & Technology – Director

Well, it sure would. And you know to the extent that there you know are some um of the larger organizations that are heading in this direction um due to kind of multiple factors, again once you sort of set a requirement that you might need to credential somebody at a higher level for one set of relatively or increasingly common transactions, it may make it hard to maintain a you know a two level, two tier system.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes.

Deven McGraw – Center for Democracy & Technology – Director

Um, but again assuming you know that you could overcome the burden issue for internal access within your own institution.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

So maybe, Deven this is a, maybe this is the way you’re already thinking about it. But –

Deven McGraw – Center for Democracy & Technology – Director

It may not be, David, so go ahead.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes. So I'm thinking that maybe what we really should be doing is assume that the correct answer or the long term stable answer is level three multi-factor all the time and what we're trying to do here is to carve out exceptions, temporary exceptions to that rule, well maybe temporary, maybe not. But let's say we're, instead of, in other words, let's not argue when we should use level three, let's argue when it's okay to not use level three.

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

Well, or here's, here's the thought, and I'm thinking about it from the, from the perspective of a VPN, if you have a VPN, an IP VPN, um the organization that you're affiliated with and that you've already authenticated yourself to, the organization you're affiliated with has already provided one form of authentication because the VPN itself has already authenticated both ends. So maybe we could say that um you know organizational authentication of a network could be one of the factors.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think that's the right way to go, and I think that's what John was saying a few minutes ago, is that if you're accessing a remote system from within a hospital where you've already had to access the hospital system you've, in a sense, accounted for a factor.

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

A factor, yes, yes, but not making an exception but allow that to count as a factor.

Deven McGraw – Center for Democracy & Technology – Director

... count?

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

That's a very conceptual way to think about it, I think.

Deven McGraw – Center for Democracy & Technology – Director

Well, I'm not disagreeing, but we sort of initially started with you know tying it to the NIST frameworks and such used in so many contexts, does that hold up? We may want to take a look.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Not strictly.

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

Strictly, right, right.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Oh, we can weave a tale that will make it make sense.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

The DEA didn't worry about it, so –

Deven McGraw – Center for Democracy & Technology – Director

Okay. Well, that may fall under the recommendation that said you know NIST needs to consider some of the circumstances that exist in the healthcare industry in further iterations of 800-63.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And I like Wes' point from the Gartner perspective of just calling this multi-factor, which is not exactly the same as a specific NIST level, but it's more than user name, password.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Judy Faulkner – Epic Systems – Founder

And I agree with that. I like –

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

... .

Judy Faulkner – Epic Systems – Founder

Yes, I like the multi-factor. I'm a little nervous about saying that we should make everything multi-factor. Well even two is multi, though.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes.

Judy Faulkner – Epic Systems – Founder

Make it NIST level three and then the exceptions be less than that because the majority of uses are going to be less and until we're sure what all the effects are means that everything that isn't, that isn't a known, so anything we're not hypothesizing now, has to be a three, and that either way there's a danger um. But I think the greater danger would be making everything we don't know to state directly three, than it would be to make it a two, because I think that the organizations themselves wanting to be secure, in other words we didn't have to say to them, as David and I just said, make your network secure. They did that. So they're going to figure out where they have to have extra for the most part and where they don't. But if we make it the rule that the default is that you have to, I think we're going to get them into trouble.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, Judy, what do, I, I mean, this is David, I understand where you're coming from there. What if we broadened the notion of acceptable carve-outs includes this notion of multi-factor. So being in the physical proximity of the hospital at a visible nursing station computer is a factor, that's a, there's a personal recognizance factor there –

Judy Faulkner – Epic Systems – Founder

Yes, but I'm not sure, unless we make sure that we say that, I'm not sure that the lawyers are going to assume that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Oh, I, are we doing anything that's legally binding, Deven? We're just doing recommendations.

Deven McGraw – Center for Democracy & Technology – Director

Well, we never get to set the law, sadly for some of us, happy for others of us.

Judy Faulkner – Epic Systems – Founder

I do think though that they interpreted it strictly as –

Deven McGraw – Center for Democracy & Technology – Director

Well, we are making a recommendation around policy, so one of the things that, either way we're going to have to be, whether we start with the premise that everything should be at a high level and we create a lot of exceptions, or we start with the premise that the basic stuff can be the low level, but the following things are written here and should be higher, you know, either way the more precise and detailed we can be, the more it's appreciated by people who might ultimately have to implement it one way or –

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I think we can kill them with detail almost instantly.

Deven McGraw – Center for Democracy & Technology – Director

Well, um, you know –

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I agree with the general premise. I just think the problem is that we can begin to talk about the differences between what affects ... and something else and yet get their eyes to glaze over if we're not careful.

Deven McGraw – Center for Democracy & Technology – Director

Right, right, right. I mean, at its broadest level we really are circling around things that are that are riskier because of the vulnerability of the network that's being used for the exchange transaction and trying to think about scenarios where the vulnerability of the of the of the exchange is addressed by one factor or another, whether it's physical presence um within a facility, um you know to the secureness of the network, you know all of those don't eliminate but greatly reduce the likelihood of the types of attacks that credentialing is designed to address, right? And so that that's essentially where the parameters we're trying to define. Um and we've made some progress, frankly, at least based on my notes. I'll obviously have to write it up and we have another chance to talk about it, but I'm just looking through the notes again for a second.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

How much more time do we have?

Deven McGraw – Center for Democracy & Technology – Director

We can stop actually about five minutes before we would move into public comment. It's only, it's a 90 minute call. If folks sort of feel spent for this call, we can, we can break a bit early and –

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

No, I was just deciding whether to, whether to –

Deven McGraw – Center for Democracy & Technology – Director

Whether to raise another –

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Whether to raise up another topic and I decided not to.

Deven McGraw – Center for Democracy & Technology – Director

Or, are you sure, because we have –

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Go for it, Wes.

Deven McGraw – Center for Democracy & Technology – Director

Go ahead.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Well, the problem is it's a little vague, as opposed to the rest of this, which is perfectly quick.

Deven McGraw – Center for Democracy & Technology – Director

...

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I kind of jumped the rails a little bit. In your last statement it seems that we're somehow talking about, well, I guess not. It, my what I was going to say is that it seems like we're somehow talking about enterprise communications at some level, but I guess when you get down to recommendations for how a physician logs in from home, then that's not inter-enterprise, so.

Deven McGraw – Center for Democracy & Technology – Director

Right, so that's right.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Never mind.

Deven McGraw – Center for Democracy & Technology – Director

And I think that the scenario that's always in my mind is that you can have trust in the HIE that you use, presuming that you use um an HIE for Exchange.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Or the HISP.

Deven McGraw – Center for Democracy & Technology – Director

Or the HISP, exactly. But how do you create the trust through the whole network, maybe we're talking about NwHIN here, where it's HISP to HISP, HIE to HIE, um without a sort of minimum set of expectations that we know all HIEs are –

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

That's why our task would be easier if we were specifically addressing what is the expectation of an authentication of a user in another enterprise who's going to interact with our enterprise based on our trust, our transitive trust.

Deven McGraw – Center for Democracy & Technology – Director

And if that's easier, what's the answer to that, because I think that is partly what we're trying to address.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, I think that's the same question.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Well, it wouldn't include standards for a physician logging in from home.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, sure, you could access your HISP from home and then turn around and use that to send a message.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

That's not the same as logging in to a, an EHR, though. That that's –

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Sure, why not? I mean a Web-based EHR, a Web-based HISP from home, either way. I think we're talking about initial access to the system and whether that system then in turn accesses another system is a different kind of problem, which is system to system trust.

Deven McGraw – Center for Democracy & Technology – Director

Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And we've covered that with our standards, we think, reasonably well, it could be revisited of course, but we're really talking about initial contact of a human with a system and what are the, what are the special circumstances that we think are enough much higher risk of an impersonation occurring that we would insist on level three. And –

Deven McGraw – Center for Democracy & Technology – Director

Or multi-factor.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Or multi-factor, yes. And I think we're comfortable that access over the open Internet is one of those cases, we're comfortable, I think, we're somewhat comfortable with access where the accessor is unable to be observed, in other words they have an infinite amount of time to keep trying, um, is a problem. Um, then beyond that it gets pretty fuzzy.

Deven McGraw – Center for Democracy & Technology – Director

Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

Okay, I yield. I yield my time to the public.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Me too.

Deven McGraw – Center for Democracy & Technology – Director

All right, well I think we'll, we will write this up and we don't have another, we're on a schedule now where we, we're trying to meet consistently, and Labor Day's going to screw this up a little bit, but we're trying to meet consistently twice a month on the first and the third Mondays, so we have two more weeks. We'll try to get this conversation written up so you all can look at it in advance. We have the meeting on the 20th to get through it, but I'm wondering if we're close enough to what we're going to be able to say on this topic that we might try to start taking on patient um authentication for, say, portal access, a topic upon which we actually did have some previous recommendations but since we're reopening the provider user recommendation we're going to see if we have reason to want to rethink what we said before on the patient issue as well. We'll see whether we can get to that second topic on our next call. Does that, does that sound good?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes.

Deven McGraw – Center for Democracy & Technology – Director

Okay. Um, Mary Jo, do you want to open us up to the public for comment?

Mary Jo Deering – Office of the National Coordinator – Senior Policy Advisor

Yes, certainly. Um, operator, would you open the lines for public comment?

Public Comment

Operator

If you are on the phone and would like to make a public comment please press *1 at this time. If you are listening via your computer speakers you may dial 1-877-705-2976 and press *1 to be placed in the comment queue. We have no comment at this time.

Deven McGraw – Center for Democracy & Technology – Director

We've flummoxed everybody. Thanks, all, for your time on this call today, and we'll talk to you in a couple of weeks.

Leslie Francis – National Committee on Vital and Health Statistics

Thanks.

Deven McGraw – Center for Democracy & Technology – Director

Thanks again.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Thanks.

Deven McGraw – Center for Democracy & Technology – Director

Bye.

Judy Faulkner – Epic Systems – Founder

Bye.