

**Privacy & Security Tiger Team
Draft Transcript
August 20, 2012**

Presentation

Operator

Ms. Robertson, all lines are bridged.

MacKenzie Robertson – Office of the National Coordinator

Thank you. Good afternoon, everyone. This is MacKenzie Robertson in the Office of the National Coordinator. This is a meeting of the HIT Policy Committee's Privacy and Security Tiger Team. This is a public call and there will be time for public comment at the end. And the call is also being transcribed, so please make sure you identify yourself before speaking. I'll now take roll. Deven McGraw?

Deven McGraw – Center for Democracy & Technology – Director

Here.

MacKenzie Robertson – Office of the National Coordinator

Thanks, Deven. Paul Egerman? Dixie Baker?

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

I'm here.

MacKenzie Robertson – Office of the National Coordinator

Thanks, Dixie. Dan Callahan? Neil Calman? Judy Faulkner?

Judy Faulkner – Epic Systems – Founder

Here.

MacKenzie Robertson – Office of the National Coordinator

Thanks, Judy. Leslie Francis, I know, couldn't make it. Gayle Harrell? John Houston? David McCallie?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Here.

MacKenzie Robertson – Office of the National Coordinator

Thanks, David. Wes Rishel?

Wes Rishel – Gartner, Inc.

Here.

MacKenzie Robertson – Office of the National Coordinator

Thanks, Wes. Latanya Sweeney? Micky Tripathi? Are there any staff members on the line?

David Holtzman – Office of Civil Rights – Health Information Privacy Specialist

David Holtzman is here.

MacKenzie Robertson – Office of the National Coordinator

Thanks, David.

Kathryn Marchesini – Office of the National Coordinator

Kathryn Marchesini, ONC.

MacKenzie Robertson – Office of the National Coordinator

Thanks, Kathryn. Okay, Deven, I'll turn it back over to you.

Deven McGraw – Center for Democracy & Technology – Director

All right, terrific. So let me just go over our agenda and sort of set the stage for what we're going to try to get done today. Uh, essentially what we're going to try to do can I, yeah, I'm just going to go to the slides here we, I want to sort of set the stage a little bit by reviewing our recommendation, at least as we sort of have it in draft to date. It doesn't mean it's final, but I want to sort of talk about where we think we've come in our discussions on this issue, which involve sort of defining the riskier transactions where we would want a second factor for authentication.

Um, and we also have with us on the line today a couple of representatives from two provider entities who have who have deployed or are in the process of deploying two factor authentication solutions. We thought that it might be helpful, particularly as we're sort of looking to think of, both finalize these recommendations and think about uh what kind of impacts that they might have on the provider community to hear just a little bit more from two entities that are grappling with this issue even as we speak. Um, and then what I hope we can do today is to try and finalize our recommendations on provider user authentication and then to do any refinements by email, because we don't have another call scheduled before the September Health IT Policy Committee meeting which takes place just after Labor Day. So it's our hope that we can since we've had a fair amount of discussion on these recommendations, be able to substantively wrap them up today hopefully using email to iron out any wordsmithing should we need to do that.

So with that, I just want to take a few moments to just summarize where we think we've come in our discussions on this issue, or where we think we've landed on our discussions on this issue over the past couple of meetings. This is not intended to be the language that I'm about to go over on these slides is going to be subject to our further discussion, so really this is just a little bit of framing. So if you'll bear with me and kind of let me get through this initially before we turn to our guests who also we have promised them that we will not try to take up too much of their time today. Um, if you'll, again, if the Tiger team members will just bear with me and let me do a little framing, we can take a couple of questions, but let's try not to jump into the substance of this till we have an opportunity to hear from our guests. And then we'll have time on our call to continue to discuss these recommendations and further refine them, with the goal of trying to finish on this call today if we can. Recognizing, of course, that if we need more time to talk about them we'll, we'll figure those things out. But that's, that's my hope.

So, where we sort of have come from is that, again, we're, we actually even got the Policy Committee to, to tentatively agree on, on, the last Policy Committee meeting that there ought to be a sort of minimum level of assurance for credentialing of three, particularly on the authentication side for riskier exchange transactions ideally for Meaningful Use Stage 3. And, in further defining what those riskier transactions might be, which we were asked to do by the Policy Committee, we, we were sort of ... around a couple of key concepts. One is transactions where, that are going to be traveling across the network, any part of which either is or could be unsecure such as the open internet or an unsecured wireless connection. Another concept that we were circling around is circumstances where a person is logging in from outside of the physical confines of an organization where they can't necessarily be observed by others. Um, since this issue is really around identity of the person and, and is it who they, who they claim to be when they're engaging in a transaction.

Then, of course, you know, again riskier transactions are part of you know identifying those is also part of an organization's security risk analysis under the security rule. Uh, and then low risk activity such as on-site intra-organizational access to systems or data, particularly where the users can be observed by others, shouldn't necessarily require level of assurance three. And that was sort of really where we were kind of circling around, but, again, we didn't, we haven't finished those discussions yet and we will be able to do so on our call today. You know, we think some of the outstanding issues are, you know, did we land in the right place with respect to the transactions that we think are riskier do we need to add to it? Do we need to take, do we need to take a category off the list? Do we need to add further clarification? What types of burdens would be associated with using two factor authentication, and how are they being managed? And—and hopefully, we'll get a sense of those issues from the, the folks who have agreed to join us today.

Um, does the—do our policy recommendations implicate a potential requirement for certified EHR systems in the next, in the third stage of the EHR incentive program, and if that's the case how would, how would such a requirement be articulated? And, and as I'm reading this off the slide it occurs to me that, you know, and is it our place to, as a policy recommending body, to make this recommendation, or is this something we should ask the Privacy and Security working group of the Standards Committee to weigh in on. And then I think maybe another issue to think about is what are the implications of you know potentially, potentially setting the bar above what the DEA requires, at least with respect to ID proofing because you know for institutional purposes under the DEA rules, as you saw on the slide, the institutions do have the discretion to be able to at least ID proof the individual prescribers within their institutions who may need to prescribe controlled substances. And we have talked as a group about whether you know in making a recommendation for LOA3 whether we want to sort of focus more on the authentication piece and, and maybe less on the NIST standards for, for identity proofing.

So I want to pause there, and I greatly appreciate the members of the Tiger team for letting me get through that framing. Um, before we ask our two guests to give us there, their, each of them, again, we have Monroe, let me just tell you who they are first: Monroe Wesley, who is the Director of Enterprise IT Risk and Informatics Security at Vanderbilt University Medical Center; and Michael Frederick, who is the Chief Information Security Officer at the Baylor Health Care System. Each of them will talk about their experiences in deploying two factor authentications in their provider setting, and there will be an opportunity for the Tiger team members to ask them questions as well. But before we turn to Monroe to start us off in that conversation I want to pause for a moment, an—and see if any member of the Tiger team has any questions about sort of our goals for the meeting, where we're taking this etcetera.

Wes Rishel – Gartner, Inc.

And you were hoping nobody wouldn't speak up.

Deven McGraw – Center for Democracy & Technology – Director

Well, well, you know what you, Wes, this is the part where I invited you to speak up.

Wes Rishel – Gartner, Inc.

Yes. I know.

Deven McGraw – Center for Democracy & Technology – Director

You're perfectly fine.

Wes Rishel – Gartner, Inc.

So, I just want to be absolutely sure when we're talking about a LOA for vetting the identity of a person and when we're talking about an LOA of authenticating them to use the system, for one thing it's not practical to have a different LOA uh vetting the user depending on how they're using the system. So now, we wouldn't, I don't think it would be reasonable to say that, vetting the vetting process. I suppose it's, you could construct scenarios where it might be necessary but overall you're not going to vet an identity's user twice, you're going to, a user's identity twice, you're going to vet on it just once. So you—you need to be very careful when we're speaking to say which kind of LOA we're referring to.

Deven McGraw – Center for Democracy & Technology – Director

Right. That's a really good point, Wes. Um, and—and that, when we, I—I suggest that when we get to this stage of, of, of getting back to our discussion of the recommendations that we—we be, we be much more clear about what we're talking about. Is it, is it pure LOA 3 for both ID proofing and authentication, or are we really sort of focused on the authentication piece?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And, and this is David, and at one meeting in the past we actually talked about kind of staging those two independently of each other just to re —

Deven McGraw – Center for Democracy & Technology – Director

Yes. We—we did, and that that we certainly can—can, we can discuss that as well. Okay, with that Monroe, are you ready?

Monroe Wesley – Vanderbilt University Medical Center – Director, Enterprise IT Risk and Informatics Security

Sure. Sure.

Deven McGraw – Center for Democracy & Technology – Director

Okay, terrific, and we can hear you just fine. Thank you. So you're going to speak to us without slides which, by the way, is just fine. I just want to make sure we weren't missing something.

Monroe Wesley – Vanderbilt University Medical Center – Director, Enterprise IT Risk and Informatics Security

Yes. Hello, everyone. I was asked to speak with you and just give you a brief history of some of the experiences that I've been fortunate and/or cursed with here lately. I started out, and the way I ended up at really getting to Vanderbilt or becoming an employee here at Vanderbilt was an association with the Health Information Exchange in the West Tennessee area. Some of you may be familiar with it, it's ... Health Alliance. And I was working in that area for an organization down there that was a participant in that. and at the time, Vanderbilt was awarded an art grant and to do this Health Information Exchange planning grant down there and actually took off and because Vanderbilt had the project management and EMR system here that was capable of getting that off the ground started to house that information here at Vanderbilt.

And as a result of the information being it's part of Vanderbilt segmented EMR, securely segmented off, that caused that to be considered remote access for anybody in the Memphis Health Information Exchange to access the back to the system here, and therefore the ... Health Alliance started out with having to go along with the policy of what Vanderbilt had, and that was that for remote access to our EMR system you would use two factor authentication. That particular vendor, and they're still in place here, was ... secure ID tokens, and we were using hard tokens at the time and continue to use hard tokens today here at Vanderbilt.

So, initially, the organization, ... Health Alliance, the Health Information Exchange organization there started out with having these two factor authentication from the very beginning, and that's just the way it progressed. We ended up with managing over 400+ users within that region and always used two-factor authentication to get into that system. To, to tell you th—did all of the providers love having the secure ID token, I would honestly say no, they did not. Uh, but in many cases we would have just about as many that might complain about having the two factor authentication as a mechanism of forcing them to get in, as many as would complain about it there would be as many that would be complimentary to being able to get into the system to get to the information.

And my emphasis there is that I had providers tell us various times and in dealing with you know here's the nuisance of having to get in or carry the token and that's usually the stigma that goes on with the two factor authentication is, you know, one of the examples was I wouldn't care if you made me jump through a couple of extra hoops as long as the information that I'm going to obtain is, is valuable. And, and, in that regard starting Health Information Exchange in that area was—it was very valuable for those that were wanting to see the information.

It and then as I wanted to tell, too, that Vanderbilt here we've been working trying to go to two factor authentication more in the normal setting and through the years being in security one of the things that's always been a struggle is the carrot or the stick. And in many cases it's kind of hard to sell some extra security items. I kind of sometimes struggle, and I shared with some of the, some of the people that we set this up with in—and earlier to ... this was—was, you know, there's this stigma with information security things sometimes is a struggle, where a physical security is just automatically assumed. And my examples for that is that very few of us ever question the fact that an office door requires a key or that we might use our security systems in our homes and lock our doors when we leave. And then the example I always use is that very few people that drive vehicles will get out of their vehicle at any point and not lock their doors. Um, but yet we want to make access to systems real quick and easy and we want just usernames and passwords. And the truth is most users would rather just not have anything and be able to get in.

And so, where I, where I say we struggle with that in some regards from a, from the security profession is that we haven't really had some of the technologies advanced, for an example, the keyless entry for your car very few of us maybe will remember the fact that we just have to walk up and use a key to unlock our doors or to unlock our cars and now we just simply push the button. And so as technologies advance and move and progress hopefully we'll be able to reduce some of those struggles and get better parallels in the information technology world. Um, some recent things that happened, some of you may have seen the fact that the wire, the *Wired* journalist here has published the fact that he got hacked very recently, and the fact of having multiple passwords and having good secure passwords, the systems in themselves and the, the different going from an iTunes password to an Amazon gave vulnerabilities there to allow somebody to hack that particular individual's, Matt Honen's information, and that's just a recent example that's happened.

So I say that, to say, okay, well where's Vanderbilt heading and what are we doing? Today we do require um, a – for our EMR if we do remote access to our network we, the application itself will recognize whether or not which IP address range you're coming from, so if you're coming from something external to the, to our known internal IP address we automatically prompt for somebody to use their secure ID token, for our users to use their, their tokens to get into the, to access the system. And where we're headed, and one of the things, and I, the reason why I bring up the carrot and the stick is, in days past a lot of us that have been focused on security would love to have two factor authentication even to our network, and we – it's a tough sell for the end users because, one, they would either have to carry a physical secure token and do something different than they had been doing for years by just putting in their password. Or two, even if you gave them the soft tokens to maybe even potentially run on their smart phones or their devices that they're carrying today you still you're, you're introducing something new to them that they're not accustomed to using and, and it's a perceived, you're slowing me down as to getting my job done.

One of the things that we have found recently and what we're going after is in trying to do more patients at a more efficient rate, getting in and out of systems and getting back into our EMR at a, at a context we've learned that we can save about 30 to 40 seconds by actually virtualizing our clinical workstations and allowing a, a provider to keep the context of where they were when they left off at one device going to the next, instead of having to log in and, and get back in to a patient's chart information. Well, in that 30 to 45 second range we also learned that for about 5 or 6 seconds it's essential that we can start to use a prox card technology two factor authentication to actually allow them to start using a PIN to actually tap a reader, let that prompt the user name and then assign a PIN associated with that and let them get in with their PIN. When they realize that they can save an additional 4 or 5 seconds, now we've got the carrot interest out there, we've got something dangling in front of them that really translates to real time, so we've got our organization excited about going to that.

We're going to incorporate that into an iCLASS smart card technology to put into our employee badges. So we're hoping, and we're just in the first stages of that, I'll admit, of potentially getting all of our users to get to a point to where at least on our clinical workstations they're starting to use two factor authentication to get in. I hope someday, selfishly, that I can actually walk in and, and just, I use an administrative style workstation and not a clinical workstation in my work to be able to use the two factor authentication to get into our network and applications as well.

So that's trying to keep it brief, it's given you a history of what some of the things we've experienced. Um, and what I'm trying to emphasize the fact is that I don't, I think it's a little bit of a tough sell. However, I also think it's very important that we get to a point to being able to have a multi-factor strong work—I actually call it a stronger authentication here just because of the consumerization of IT many organizations wanting to be able to support the bring your own device to work. I think it's going to a point to where we're going to be much more focused on who you are accessing systems rather than what devices you're accessing on. And in order to do that I think that multi-factor authentication is going to become more and more important to keeping individuals straight and improving. So trying to keep it brief, hopefully I condensed that and can at least give you an idea as to where we are and some of the things we're looking at doing. With that, I'll turn it back over to the moderators.

Deven McGraw – Center for Democracy & Technology – Director

Okay. Thank you, Monroe. That was—that was terrific. And do you have time to remain on the call?

Monroe Wesley – Vanderbilt University Medical Center – Director, Enterprise IT Risk and Informatics Security

Oh, absolutely.

Deven McGraw – Center for Democracy & Technology – Director

Okay, great.

Monroe Wesley – Vanderbilt University Medical Center – Director, Enterprise IT Risk and Informatics Security

I planned that, but I didn't want to run over time and –

Deven McGraw – Center for Democracy & Technology – Director

No. Which we greatly appreciate it because I think we're going to turn to Mr. Frederick's presentation. Um, but if we are able to have you both on the line for a bit, because I suspect that there will be questions from Tiger Team members that, that would just be terrific. So if you just want to wait for a minute, we'll let Mr. Frederick talk to us about what's going on at Baylor and uh, and then we'll have a, have a discussion.

Michael Frederick – Baylor Health Care System – Chief Information Security Officer

All right, well, I did happen to send in some slides, although I'm not going to walk through those slides. The slides are for your information in order to just give an overview of the solution that we are piloting here at Baylor.

Deven McGraw – Center for Democracy & Technology – Director

Oh, terrific.

Michael Frederick – Baylor Health Care System – Chief Information Security Officer

There's some information in there as to the level of vetting for the different level of credentials. Um, we are remarkably similar at least our story is to that of Vanderbilt. Um, I got here about eight years ago. Um, in a previous life I did about 15 years of security consulting. And then I worked with a couple of major airlines here in the Dallas area, one of which is now in bankruptcy, but, and the other one was Southwest, before coming into healthcare for the first time. And it was a bit of an eye-opener from a security and privacy standpoint. Um, when I got here HIPAA had been around for about nine years, I guess since '96, I got here in 2004/2005 and the state and level of compliance was, well, shocking to say the least. Um, we did have a policy on the books for remote access at that point in time which required two factor authentication to any information that was classified as internal use only or confidential. And here at Baylor we have a three tier system - it's either public information, internal use only, which is for Baylor employees use, or confidential, which is private.

And, we also have the, the hard tokens from RSA, and there was great resistance in the physician community to using those. Uh, one of the arguments that they threw out there was, well, if everybody required this then I would be carrying around 30 of these tokens, much like I have 30 physical access badges for everywhere that I practice medicine today. Um, and, of course the, the time to log in was a factor as well. And as part of those conversations, we started talking with HITRUST and several other organizations that were participating in HITRUST in the creation of their common security framework about the problem we were having. And we found that there was some common needs out there, something that is highly flexible, that can be vetted to different levels per the requirement and per the level of identity that that the person was going to present. Um, and through further conversations getting some technical folks involved it, it began to become clear that, that we had a shot at designing something that might be able to address the concerns of the physician community, and that those conversations morphed into what is the HITRUST ID today.

And, the HITRUST ID was designed to be your password or identity as a healthcare practitioner. Uh, there's, there's only one of you in the physical world we believe that there should only be one of you in the logical world. Um, so you know, and as, as systems are becoming interconnected and information is moving being able to track who is doing what, with what, and where that, that universal identity is, is going to become more important. Um, we have gone through one pilot phase, and my apologies, I didn't send it in time to have it attached as part of this presentation, but I—I did send the results survey results of the physicians that participated in, in the pilot that we did back end of June, early July time frame on the usability the acceptance level, and we asked them to rate the experience and the product several different ways from one to five, one being lowest, five being highest and everything averaged out at about a 3.5. Um, that's everything from getting the identity setting up the application on your iPhone, and the ability to use it to sign in so those results were encouraging. Um, we have taken some of the feedback that we've received in that pilot and we are now working with the folks to make it even more palatable from a physician standpoint.

I personally, as a security practitioner for 20+ years, think that two-factor is the way to go. We've also taken steps here at Baylor to virtualize our clinical workstations. Um, the original design was to go with a card-based system not exactly a prox system but something where you had to physically insert the card. The, the security trade-offs with that model in our estimation w—was that it would enable us to do some things around timeouts that we couldn't do if we didn't have something persistent at the machine. Um, there has been resistance to that when people figure out that the same card that they used to access the PC is also the one that opens doors throughout the facility, and they are shocked to find out that they cannot leave the card in the machine and be able to walk around in the facilities and leave their machine logged in. The radiologists tend to be the ones to complain about that the most because they like to take breaks and leave everything up and logged in and they expect it to be there when they get back. Um, we haven't had any great success in getting any of the radiology reading stuff to virtualize, so we're stuck with the native functionality and, and it makes it hard to get that model.

What we have found in that model with user name and password, as we start to get calls about workstation performance when our field services folks get to the machine we find out that there's 35 different EHR sessions that are there. People are not disconnecting, they're not logging out you had people clicking on the wrong session, we've had increased instances of what's called session stealing, where somebody gets into somebody else's session and—and it, it becomes a mess. And so, we're, we're looking for ways to clean that up within our environment.

Just from a remote access standpoint the main risks that we've had up to this point in time has been a privacy or identity theft risk to our patients. Most of the information that physicians get when they came in remotely was read only. What we're finding now rolling out the EHR providing remote access with online order entry they're able to actually input orders remotely which gives them, or whoever is on the other end of that connection, the ability to actually affect people with what occurs while they're in one of our facilities. And so you know in my view the risk has gone up one more level for the remote access. And being able to do something that gives me a higher level of assurance that you are who you say you are is, is going to become a patient safety issue, in my estimation.

The other thing that's rampant because my team gets these calls from the help desk it is quite common for a physician staff to call in to try to get a password reset. Um, those are escalated to my incident response team and they have the fun task of, of calling the physician's office and educating them on proper password etiquette and that they're not to be shared. Um, and there are some physicians that get downright angry and rude and make comments, bold comments, as, "I will continue to share my password, thank you very much," um, and, and go about their day. So you know when you look at the amount of password sharing that occurs with the, with the physician, at least what we've what we've seen when you just look at the security threats out there, talk to a Symantec, McAfee trend whatever your vendor du jour is with the malware you'll find that, that probably 50% to 60% of the PC's that are out there on the internet home users are probably infected with multiple forms of malware and a high probability of having keystroke logging capabilities on those.

So, you know, now you get to a situation where passwords are easily stolen remotely in a non-controlled device couple that with the amount of password sharing that occurs and there's not a high degree of confidence that the person on the other side of the keyboard is the person that they say they are. And then you add the abilities to get into the EHR and, and tell somebody in a hospital to do something to a patient and that becomes even more frightening from my standpoint. So but we are diligently working with our physician community to try to get this to a point where it you know is doable for them to where they won't complain too much but I think you know if you get a chance to review the results of our survey we had a 60% affirmative both or feedback on the solution we're trying to roll out, a—and we're, we're hoping that it will only go up from there. So that's my presentation.

Deven McGraw – Center for Democracy & Technology – Director

Okay. That's ... that's terrific, Michael. We—we greatly appreciate it. While we have the two of you on the phone I'm going to open up the floor to members of the Tiger Team who want to ask you some questions. Um, is there anybody out there who'd like to go first?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Deven, this is David. I just have a clarification question for Michael. When—when they took that survey and you reported those results what was the actual process they were using to log in that they responded to in the survey? I—I wasn't, you, I'm sure you said it. I just missed it.

Michael Frederick – Baylor Health Care System – Chief Information Security Officer

We use a Citrix NetScaler device to provide virtualized apps and access into our EHR, and so they're coming in through that environment using the HITRUST ID on their smart phone.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

So they're doing it a secondary PIN sent to the smart phone at each log-in?

Michael Frederick – Baylor Health Care System – Chief Information Security Officer

Uh, yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Okay. So not, you were not using the, a tap card, prox card approach at that point?

Michael Frederick – Baylor Health Care System – Chief Information Security Officer

No.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Okay.

Judy Faulkner – Epic Systems – Founder

This is Judy. What percent response did you get?

Michael Frederick – Baylor Health Care System – Chief Information Security Officer

Um, we had 35 physicians participate, and 23 of them responded to the survey.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, we're going to – we'll get that on, this is Deven, we'll get the survey distributed to all of you that Michael sent it, sent to me by email.

John Houston – University of Pittsburgh Medical Center – Vice President, Privacy & Info Security

Hey, Deven, this is John Houston. I'm sorry I was late.

Deven McGraw – Center for Democracy & Technology – Director

That's okay. Hi, John.

John Houston – University of Pittsburgh Medical Center – Vice President, Privacy & Info Security

How are you?

Deven McGraw – Center for Democracy & Technology – Director

Good.

John Houston – University of Pittsburgh Medical Center – Vice President, Privacy & Info Security

Great. I had one question you talked about some of the physicians, I'm going to call them satisfaction issues that you know engaging physicians and, and some of those challenges. What's the strategy to try to, to make this more transparent to them or what do you—I mean, do you think this is going to be an ongoing burden with your physician community?

Michael Frederick – Baylor Health Care System – Chief Information Security Officer

Well, in the Dallas market as with any large market we have a pretty competitive environment, that that has really been the item that has held security back. Um, because anytime you take a step forward from a security or privacy standpoint you're running the risk of costing yourself business because there's another system across the street that doesn't see it that way or doesn't do it, and it—it can be frustrating at times. So the approach we've taken is to try to partner with the physicians and try to overcome any of the negative connotations or feedback that they have related to the two factor solution.

John Houston – University of Pittsburgh Medical Center – Vice President, Privacy & Info Security

Well, I understand. I guess my point was more philosophical. Are there strategies you see on the horizon that will allow you to make this more transparent to that physician community such that you don't have that, that, that push back that you—you're experiencing, or is that still a—?

Michael Frederick – Baylor Health Care System – Chief Information Security Officer

Yeah, you know, the, the application that runs on the phone it is—is becoming better. Um, today we force authentication to the phone so that we force encryption of the phone and then the application requires a separate PIN. Um, in the next coming version of that if the phone is password protected you're not going to have to input a PIN to generate the code so that just removes, you know makes it easier to use. Um, so yeah, yeah we're—the technology is evolving, but you know, it's not quite to the point of the car analogy that was used earlier where you can just press a button.

Deven McGraw – Center for Democracy & Technology – Director

Mon—Monroe, did you have an answer to either of those questions or want to chime in?

Monroe Wesley – Vanderbilt University Medical Center – Director, Enterprise IT Risk and Informatics Security

Well, I think one of the interesting things in, in hearing this presentation as well is Vanderbilt being a little different we, the majority of the providers and staff that we have here are Vanderbilt employees. so we do—and not to say that we don't have some that float in and out of other organizations and—and I'd be referencing carrying the 30 different IDs, and one of the things that I found out true in the health information exchange world and doing it at a regional level in West Tennessee down in the Memphis, Tennessee area, was that you know the providers tend to carry around a book and they have their user names and passwords written in them for every organization that they work in. And heaven forbid if they ever lose that that book.

And that scenario, very much to what's been described here from—from Baylor and trying to do it at a more what I would consider a kind of a regional level is very I guess that I'm very optimistic that that'll continue to go. And it's very exciting to hear because we've started talking at the regional level of maybe getting the providers to log to—log into the authenticate to the centralized or the health information exchange context and then ask if the participants out there start to use that as a trusted way to allow a provider to get in, so then maybe they could get to just the one ID and then be trusted to get back into their own individual systems. So I think that context is, or that approach is very, very exciting to hear. I want to read more about that and learn more about that, and actually, wouldn't mind having a conversation offline after this because I'm excited to hear that.

Uh, one of the things that I—I've said here that Tennessee being one of those states that's spread out geographically, the only one in the United States that touches eight other states we're spread wide so it's kind of hard to do it at a state level, but I've often said you know it'd be nice if the state would give the providers and those that are in the healthcare industry that have to pay licenses and their fees, maybe give them an idea at the state level and help try to track the individuals from just an authentication and a proofing standpoint, would be very helpful. So that's the only comments I have. I think, you know, where Vanderbilt might be just a tad bit different is, is, our, our user mix is a little bit more dedicated here, so our employee badges ... to try to implement the two factors.

Deven McGraw – Center for Democracy & Technology – Director

And both of you really, this is Deven, initially focused on remote transactions for multi-factor authentication. That—is that right, and now you're, you're in various stages of exploring multi-factor for workstations, virtualized work—virtual workstations in a clinical setting. Is that right?

Michael Frederick – Baylor Health Care System – Chief Information Security Officer

Yes, yes. So, for inside the organization, it really becomes a utility. So the DEA has certain requirements for being able to ePrescribe and they become elevated when you're talking about controlled substances. And in our ambulatory setting we're in conversations right now to try to be one of the first to be able to do the controlled substances because it's very aggravating and—and as a parent with a child that has ADD to get all of the prescriptions electronically sent to the pharmacists except for this one where they hand me the green piece of paper and I've got to go drop it off anyway. So, they really haven't saved me any time from, a, from a patient standpoint, and so we're looking at being able to do that. That's going to require a level of two factor authentication. There's, there's also some other security trade-offs that can occur if I have a higher level of assurance and I can be assured that your session is going to go away when you walk away I can start to remove or loosen some of the other constraints that providers find aggravating. So that's where we're starting to look at it on, on ways to apply it inside the network.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, yes, this is David. I wanted to follow up on that. You, you had rejected the prox card approach initially because you wanted to have a, you know present a way to measure whether they were still present at the workstation, and then that created its own problem when they forgot to remove the card or when you couldn't virtualize the sessions for the radiologists. Are—you, are you willing to go back and rethink the prox card approach, that maybe that could be secure enough and solve the persistent session problem some other way?

Michael Frederick – Baylor Health Care System – Chief Information Security Officer

Potentially. Uh, there was another organization here in town that went that approach and found that there were some very crafty users out there that were able to use that proximity, an—and their badge to be able to do things that they didn't want them to do. And when we're—when we're looking at the controlled substance standpoint you know you have to have a federal bridge level cert which these cards that we're rolling out are actually smart cards with the chip in them and you've got to be able to read the chip to get the cert off, and it's not something that can be done in a prox. But certainly for just pure authentication to a workstation to get a session going, we would be willing to look at that. But, but when you need to get the cert off the card that prox proximity doesn't exactly work, you've got to have the card in contact with the reader.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. Although, I thought they were ways, well—we, I don't think we want to get off into the DEA thing.

Michael Frederick – Baylor Health Care System – Chief Information Security Officer

Yeah.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Okay. That helps. And one other, wait a minute — oh, never mind. I've lost my train of thought. I'll let someone else jump in.

Deven McGraw – Center for Democracy & Technology – Director

Come back, David. We'll see if someone else has—

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yep.

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

I have a comment, this is Dixie, an—and a question actually. It's interesting to me that Monroe mentioned that they always have used two factor authentication and the—the doctors thought it was, it was okay to jump through hoops as long as the information was valuable to them. And Michael also said that this two factor is an—they're implementing it as a way to do ePrescribing of controlled substances. You know in both cases when, when the two factor is introduced it provides the doctors a new service or new value that they didn't have before. And I'd be interested in knowing wha—how much you think, or whether you'd get that same result if, let's say, in Monroe's situation if you, if you had already been allowing them to just log on and then you, and then you said one day we're, we're strengthening this by adding a, making it two factor, do you think you would've gotten more pushback? I mean, you know, that context of introducing, how important do you think that context of introducing two-factor as you introduce a new value to them is in the acceptance equation?

Monroe Wesley – Vanderbilt University Medical Center – Director, Enterprise IT Risk and Informatics Security

I would say it's very strong in the fact that I think it's a tough sell it kind of goes back to the analogy that I'm using with the keyless entry to the cars. I believe because we were we're at such a point the information technology security world of just being so programmed to user name and password that we've got this thought process in our head that two factor takes longer. When the truth is once you get used to using it, it can be uh, as quick and in some cases at least as quick as a user name and password in typing so I think it's very important that you try to do that.

Now, we had a remote access policy ... that if you were going to do a remote access you're going to use two-factor. And then on campus, until we got to a point to where we could introduce the—you could actually get on about four to five seconds quicker than the average typer could do their user name and password, that's where the attractiveness came in. And just one point of clarification on our proximity cards we're actually we're tapping—we're getting close enough to the reader to have it read, so we've got that distance turned way down. We don't have the interference of multiple users walking up to the workstation and it being at a distance. So it's actually more of a you've got to get close enough to, for the card to actually read, and then I didn't want everybody to think that it was, you know, standing back at a distance, just for clarification. And I'll, I'll let Michael respond.

Michael Frederick – Baylor Health Care System – Chief Information Security Officer

You know, any time that you meet resistance anytime you ask a physician to do something that they're not doing today. Um, and obviously the way, the best way to overcome resistance for anybody is to you know offer something, a give to the take, right. Um, I kind of draw an analogy from 25 years ago or so when word processing in the PC started to become a, a business tool. You know there was a point not long ago where everybody at a director or above had an admin assistant that typed all their memos and, and did various things for them, and, and the PC and the word processor allowed organizations to reduce that cost um, and put that more of the burden each of us.

And, you know, I can remember my parents were still in the workforce in those days and, and it was like oh my gosh I'm having to type my own stuff now and I'm—I'm so much more inefficient, and physicians are kind of going through that same evolution. So their—their workflow today, they're used to, they're used to shouting out orders, they're used to doing things over the phone, they're there's not a lot of high touch actual data entry type stuff that they have historically done in their workflow, and this is probably the reason why so many of them pass out their passwords so that their staff can log-in and do the things that they used to do in the paper world as far as retrieving charts and, and that type of stuff. And so you know they're, they're going through a fundamental shakeup of their workflows and, and they're being asked to, to interact and do things that they used to pay others to do. And you know they need to get something out of it when you throw another requirement at them.

But that being said, you know, the big obstacle that we've had here is the fact that not all of the systems require it. And when not all the systems require it, you know, if you point to HIPAA, HIPAA just says do a risk assessment not a lot of guidance on how that risk assessment goes and then you get yourself into, into a circular conversation with a physician over what exact risk goes into that measurement. Um, if you talk to a physician inhibiting their access to information potentially puts the patient at risk. Um, you talk to a security person and it's all about assurance of who's on the other end of the keyboard. Um, is it somewhere in the middle, is there a balance, what exactly are we supposed to be protecting and you know I would like to get it—to get it to the point where it's a lot more uniform, that there's not 40,000 different ways or answers to the question. You know a handful is probably enough that gets everybody into the same ballpark and that would make the security job a lot easier, so.

Monroe Wesley – Vanderbilt University Medical Center – Director, Enterprise IT Risk and Informatics Security

Great comments.

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

Yeah, yeah, that's, yeah.

W

It's very, very helpful.

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

If they're – not all systems require ... is perceived as arbitrary.

Michael Frederick – Baylor Health Care System – Chief Information Security Officer

Correct. And I think the risk assessment is you know what's the assurance of the person on the other side of the keyboard being who they say they are and what are the risks. And I think with, at least with remote access based on the malware the known password sharing, the books that are carried around with passwords in them, you know, when you get off network that assurance level drops to a low to medium at best.

Deven McGraw – Center for Democracy & Technology – Director

And remote...

Monroe Wesley – Vanderbilt University Medical Center – Director, Enterprise IT Risk and Informatics Security

Vanderbilt...

Deven McGraw – Center for Democracy & Technology – Director

Oh, I'm sorry. This is Deven again. By defining remote as I sort of took this down I think during Monroe's presentation a—an IP address external to the system. How would you define remote?

Monroe Wesley – Vanderbilt University Medical Center – Director, Enterprise IT Risk and Informatics Security

Yeah. For us, because our, you know when you start thinking about academic medical center and the fact that our network spans over, well, over the city, so, and—and remotely so. So when we say that we say outside of our network, and that's why I said an external IP to our known IP address ... internally. And we just have a different level of assurance, I agree exactly with Michael, we'd have a different level of risk with something that is outside of our network versus something that we've done more trusted inside our network.

Deven McGraw – Center for Democracy & Technology – Director

And, Michael, how about you would—do you have—how do you define remote?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Hey, Deven, could you have, could you say that last sentence one more time? So I—I think I misheard or heard it and I want to make sure I heard it correctly.

Deven McGraw – Center for Democracy & Technology – Director

Oh, go ahead, Monroe.

Monroe Wesley – Vanderbilt University Medical Center – Director, Enterprise IT Risk and Informatics Security

Oh, I was just saying that we—our network is something, you know, we're spread out all over—all over the city here in various buildings, so we, anything that we deem outside of our network is outside of our internal IP space, so and we have our different risk level of—and a different level of assurance of devices being a little bit more trusted, secure, however you want to phrase it we have a different level of risk posture and a different level of assurance of, of the devices internally versus the ones that are external. Very much like what Michael was saying, you know you're concerned about having that level of assurance who's trying to connect to you remotely, so.

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

Do you have any wireless connections to those IP addresses? How do you know they're wired

Monroe Wesley – Vanderbilt University Medical Center – Director, Enterprise IT Risk and Informatics Security

Our—our wireless, actually our wireless activity is 100% authentication. We don't allow anything to sit on our network at all unless it is an authenticated user, so we do treat our wireless base totally different than we do our wired.

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

Thank you.

Michael Frederick – Baylor Health Care System – Chief Information Security Officer

So, Baylor's definition is the same as Vanderbilt, with one caveat. Um, we do have—we do offer our visitors free wireless Internet access and we do have providers that bring their own device that hop on that. Um, that is also considered outside our network. It, it does not ride on the production network and all of that connectivity is routed out to the internet before it comes back in, if they're trying to hit an internal core production application, so we treat anything from that visitor wireless as untrusted as well.

Deven McGraw – Center for Democracy & Technology – Director

Got it. Any other questions for these two gentlemen before we let them go?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

This is David. I have one more question. Just along the lines of the physician attitude issues that both of you identified, I—I know it's just speculative but do you have any idea what the DEA requirements will do that might affect the way people think about second factor authentication? I—I assume most of your physicians will at some point have to go through that process because they will be writing for controlled substances. Is that going to change the level of expectation in a year or two?

Monroe Wesley – Vanderbilt University Medical Center – Director, Enterprise IT Risk and Informatics Security

Uh, potentially, you know, I guess it all depends on the volume of that type of prescribing that a physician does. Um, you know as it sits today we don't have anybody that's prescribing that way, and our EHR vendors don't even—don't even have that functionality built into their products yet. So we're still working with them to try to fast-track some of that. So, I think—I think it will because at that point you have a definitive requirement that if you want to do “X” you must do “Y,” um, and when you get those types of requirements you get much less pushback.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. Yeah, that's what I'm—I would guess. It may change the expectation level. One, one last question, I remember now what I was trying to remember before.

Deven McGraw – Center for Democracy & Technology – Director

Good.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Which is, and I think you touched on this, but do you do anything about the context in which the physician is accessing the system even if it's internal? You know you're clear what you do for the external access, but for example, this is a terminal that this physician has never used before, first time use, or maybe something that pays attention to the hours of use, something in the middle of the night might be treated differently than something in the middle of the day, do you factor any other context dependencies in the decision whether to request a second factor?

Michael Frederick – Baylor Health Care System – Chief Information Security Officer

Uh, at, at Baylor we do not. W—we are looking at some of that for the external connectivity to where maybe if you're coming from a known device like your home station that you've registered much like your bank does, then maybe it's only once every 30 days that we ask you to re-register that device ways to still get the levels of assurance and not have to have the second factor every time. Um, but in—inside our network, no, we, we do not do any of that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Thanks.

Monroe Wesley – Vanderbilt University Medical Center – Director, Enterprise IT Risk and Informatics Security

And as far as Vanderbilt's concerned our clinical workstation environments are managed a lot tighter than our administrative workstation environment. We do have some providers that will access from both, so we do have a little different approach there as far as, and the easiest way to describe that is our clinical workstation environment really is kind of more of a single sign on to some of our multiple applications, our clinical applications that we have. And, and that is just because of ease of getting on to the actual physical network a little quicker and registering users. So, but in that context only and—and we're looking at, at a lot of different things of wanting to monitor session access.

What's—honestly, the sharing of passwords concern I've kind of sat over here and chuckled at a lot of what Michael's had to say because we've experienced a lot of the same problems, and I think we're not—and neither one of us are probably independently unique, but in that that's one of the things that's helping drive us to a virtual clinical workstation environment. We'd really like to get to a point to where a provider or user, for that matter really deals with one session and we have one session in the system per user and can't have that possibility of two sessions and a physician being at two places at one time because they're sharing their information with somebody that's helping them do their work, so. And I'm not just blaming physicians, I would just say provider in general because it's not just physicians.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Thank you.

Deven McGraw – Center for Democracy & Technology – Director

Any other questions? All right, well—well, you all are keeping with the timing on the agenda just about perfectly here. I want to give our thanks again Monroe and Michael, for your taking the time to, to talk to us today. It's been extremely helpful. Um, and uh, again Michael we'll make sure that your survey data gets circulated and our—and you have our thanks, very sincere thanks.

Michael Frederick – Baylor Health Care System – Chief Information Security Officer

Hey, Monroe, would you mind giving me your email address and I'll shoot you an email and we can have that offline conversation if you'd like?

Monroe Wesley – Vanderbilt University Medical Center – Director, Enterprise IT Risk and Informatics Security

Yes. It's just, and I don't know if we can handle that maybe through–

Deven McGraw – Center for Democracy & Technology – Director

Yeah. You know, we, we can actually connect the two of you together through an e-mail.

Michael Frederick – Baylor Health Care System – Chief Information Security Officer

Perfect.

Deven McGraw – Center for Democracy & Technology – Director

So you don't have to pass that on the phone call.

Michael Frederick – Baylor Health Care System – Chief Information Security Officer

Yes, ..., sorry.

Monroe Wesley – Vanderbilt University Medical Center – Director, Enterprise IT Risk and Informatics Security

That would be great.

Michael Frederick – Baylor Health Care System – Chief Information Security Officer

I forgot about that aspect of it.

Deven McGraw – Center for Democracy & Technology – Director

We'll take care of that for you.

John Houston – University of Pittsburgh Medical Center – Vice President, Privacy & Info Security

And a security officer at that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah, how about that?

Monroe Wesley – Vanderbilt University Medical Center – Director, Enterprise IT Risk and Informatics Security

Well, also in light –

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I don't think you should share email addresses. You should share passwords now over the phone.

Monroe Wesley – Vanderbilt University Medical Center – Director, Enterprise IT Risk and Informatics Security

Yeah. I would like to thank all of you for taking on and tackling this as well, because it's not something that's easy and it's – making a change and something as drastic as—as just user name and password and trying to get people to think more about a stronger authentication, is a struggle, and anybody else that's helping other than information security types out there it's—we're very appreciative of that. So thank you for—and it's a pleasure to be able to share this with you. I don't know that we maybe helped to answer anything, but if nothing else maybe we generated some more question and we can continue the dialogue.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

Monroe Wesley – Vanderbilt University Medical Center – Director, Enterprise IT Risk and Informatics Security

Thank you.

Deven McGraw – Center for Democracy & Technology – Director

Thank you very much.

Michael Frederick – Baylor Health Care System – Chief Information Security Officer

Thanks.

Deven McGraw – Center for Democracy & Technology – Director

All right. So, Tiger team members can't go anywhere yet. Um, so I'm just going to take us back to the sort of straw recommendation in light of—of the presentation that we just heard and also Wes's earlier comment about, you know, sort of are we focusing enough on authentication really versus sort of ID proofing, you know, calling, calling for higher level of ID proofing whether—in an, whether ultimately or in some—are we calling for a higher level of ID proofing in addition to authentication for certain types of transactions versus focusing more on authentication. Um, one option of course being one that we had talked about previously which David mentioned which is t—to sort of get first to the multi-factor authentication and then look to get to level of assurance three for both ID proofing and authentication over—over maybe a longer period of time.

But, but again, both—both of our presentations today focused on. focused first on remote with—with you know sort of definitions of remote being outside the network with, with outside of the IP space with an IP address out that, that isn't part of the system, or using an Internet-type connection in order to connect. So again, I—I want to sort of get feedback from folks about both the language that we've got in this recommendation, where, where, where we think we should be taking it from here given, given what we've just heard as well as the testimony that we had in our original hearing.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Deven, I have one comment, and I'm curious to know whether it's intentional or accidental on your part.

Deven McGraw – Center for Democracy & Technology – Director

Uh-oh.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, I mean, it makes a difference, so ye-I assume it was intentional.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

But you defined in bullet point two the way that's worded such riskier transactions “are” those. I wonder if you meant “include” those?

Deven McGraw – Center for Democracy & Technology – Director

Uh, I think that's much better phrasing, yes, David, because you know in actuality we—I think we have a judgment call to make as a Tiger team. Do we sort of set a minimum floor for the sort of transactions that we think ought to at a minimum require a higher level of authentication and then of course institutions would be free as part of their security risk assessment to define additional types of transactions for which they would require more.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Right. And I'm—and the other direction as well in that there may be risky transactions that we have failed to identify that should eventual—that should be part of the security risk assessment. In other words, we're offering guidance here, not a rule. That's really the question, I suppose, rather than the subtle wording ...

Wes Rishel – Gartner, Inc.

This is Wes. Um, ...

Deven McGraw – Center for Democracy & Technology – Director

Yeah. I think we could—it would ... you know the slide saying are those was not an intentional, um was not intended to be to try to create an exclusive sort of list of transactions that would be risky. So I—you know, certainly include those was sort of more of what we were, what I was proposing.

Wes Rishel – Gartner, Inc.

Okay. And I know—I know this is old ground that we have gone over before I'm hopeful that I haven't simply forgotten something but right now as I read this if a admitting clerk updates the room that a patient is in and that gets sent across the HIE, well, ... discharges a patient and that gets sent across the HIE, that would not require an individual user level credential because it's not a risky transaction. And, if a blood result comes back from the laboratory and a copy of that is dispatched to the HIE, will that then require that the transaction was signed individually? I know that the data content of the transaction identifies the—the certifying provider, but that doesn't mean that – I, I guess I'm wondering, are we saying that, that such transactions to be sent across the HIE must have been created from user input in a system where there was this level of validation, or are we saying some—something different? Uh, you know, it's just a whole issue of are we talking about the HIE or are we talking about the system here?

Deven McGraw – Center for Democracy & Technology – Director

I think what we're talking about, Wes, although I—I, I think I don't fully understand your question, but I'm going to try to answer it anyway. What we are talking about is when organizations should be required to use multi-factor authentication in order to authenticate a user of—of a system. So if you think about it in terms of a provider organization the—based on sort of the, the definitions of sort of riskier transactions that we think would necessitate a greater level of authentication than user name and password, they are those that come from the outside who are passing across a potentially unsecure network.

Wes Rishel – Gartner, Inc.

Okay. So that is completely consistent with the second major bullet. My confusion comes when I compare the first major bullet to the second major bullet and it says, “riskier exchange transactions.”

Deven McGraw – Center for Democracy & Technology – Director

Yep. Okay. Yep.

Wes Rishel – Gartner, Inc.

And I think that and here's how I think I recall it, recognizing I have a little confidence in my own memory I think I recall that we would ideally think that our recommendations as described in bullet two should apply to every time a clinical system is used and the system with protected health information is used regardless of whether the data actually is intended, or, regardless whether data may fly—may pass over an HIE as a byproduct of the use.

Deven McGraw – Center for Democracy & Technology – Director

Oh, absolutely.

Wes Rishel – Gartner, Inc.

All right. Okay.

Deven McGraw – Center for Democracy & Technology – Director

Yes. So –

Wes Rishel – Gartner, Inc.

So then I, I, this phrase for “riskier exchange transactions” is, is really very confusing.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

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

Yeah. I think, I think, Deven, in, in going back to where what Wes said to begin with, where in the midst of his question he mentioned digital signature, I—I think we absolutely in that first bullet need to capture that we're talking about authenticating the user.

Deven McGraw – Center for Democracy & Technology – Director

Yeah. Absolutely. Yeah, we've gotten a little shorthand here because we're, you know, several conversations into this, but that is causing confusion and we don't want to do that.

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

Yes. Yes.

Judy Faulkner – Epic Systems – Founder

This is Judy and on the second bullet there it doesn't seem to match, if I understand it correctly, with what Bill was saying, which is when we said what is your area, he said that they have different buildings around the city and that it is that whole city area that he considers his area. If I read this it says that he has to consider each physical confine.

Deven McGraw – Center for Democracy & Technology – Director

Oh, okay.

Judy Faulkner – Epic Systems – Founder

And –

Deven McGraw – Center for Democracy & Technology – Director

So not well worded, and that was Monroe.

Judy Faulkner – Epic Systems – Founder

Oh, I'm sorry. Okay.

Deven McGraw – Center for Democracy & Technology – Director

Okay. Um, it's yeah, I mean I think outside of the physical confines is, maybe isn't the right word. Outside of the net—of the organization's network.

Judy Faulkner – Epic Systems – Founder

Yeah. The organization secure network I think is really what they're talking about.

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

Or, or, or use theirs about their recognized IP address, you know, the IP addresses that the organization owns.

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

So this is David. I thought that second bullet point was actually about the security that's created by physical presence in a, in a setting where you're supposed to be.

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

Oh, yeah, you're right. That's –

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Which is completely –

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

... observed by others, yeah.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Right, right.

Judy Faulkner – Epic Systems – Founder

Right and that's a—that's really interesting because he—he did say and I think that we see it all the time, you have building, and building, and building, and building of people ... between them.

Deven McGraw – Center for Democracy & Technology – Director

Well, right. So I think what we'll—good point Judy. I think what we were meant to say here is if you're sort of logging, you're logging in from home or you're logging in, say, remotely like from an airport where you're outside, so I would—outside of the physical confines being, you know, any building where somebody else can see you log in that's part of the organization. So it may be multiple buildings but they're all part of, in Monroe's case, of the Vanderbilt Health Care System.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Isn't that completely covered by the first bullet?

Deven McGraw – Center for Democracy & Technology – Director

Maybe it is.

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

I think the second one we are talking about observed, and I think we should reference the physical—the area that is physically protected by the organization.

Judy Faulkner – Epic Systems – Founder

It would be interesting to ask Monroe if in fact as people go from one physical location to another he wants them to still be able to have access as they walk. So in other words if they're looking at their information as they're going back and forth, is that okay?

Deven McGraw – Center for Democracy & Technology – Director

Well, I think they're trying to do that with—within one clinical building through the virtualization of the clinical, clinical workstations, but they're not, they're not there yet. That's the prox card.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

But that, I mean, Judy's point is a good one that, you know, you, you could be legitimately authenticated and then while you're still running that session on your tablet device walk to a physical different building.

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

Yeah.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

But in all those cases you're covered because you're inside their network.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Judy Faulkner – Epic Systems – Founder

Right, that's what I meant because I see that happen all the time.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

You know, I'm not sure that physical—the physical observation thing is that relevant. On the other hand, Monroe did suggest that they treat the clinical computers differently from administrative computers, which you know was in part which ones are going to get virtual sessions, but I think it was also a little bit in part that it's unusual for clinicians to be accessing the system from an administrative office computer, which is a little bit of a physical proximity because obviously those are both inside their network. And I don't think we should be prescriptive here is wha—where I'm really headed, if this is all part of a risk assessment.

Deven McGraw – Center for Democracy & Technology – Director

Well, it is except that we're trying to set some minimum criteria about when we would ask—we when, I mean we're trying to tell ONC to move to multi-factor authentication for certain types of, of, of access to health information, and, you know, where we're going to do that we do need to try to be more specific than to just leave it up to the risk assessment because we're trying to raise the floor.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

So maybe the, the, the minimum or the floor is this network definition inside the network, outside your network, and the wireless secured, unsecured wireless, and then beyond that it's risk driven.

Wes Rishel – Gartner, Inc.

So, um –

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I wonder –

Wes Rishel – Gartner, Inc.

I'm, I'm –

Deven McGraw – Center for Democracy & Technology – Director

That could be. Wes?

Wes Rishel – Gartner, Inc.

You know, it used to be that ... devices were big and clunky and, and you might argue that there's a difference between a big clunky device on the nursing station or in the doctors' lounge and a big clunky device that's somewhere down a hallway and around the corner where nobody ever goes or in an individual doctor's office. Um, but I just don't know that that distinction holds up. And I particularly think that that whether the user can be observed or not is really hard to, hard to, to sustain as we are getting, you know, as we are already using devices that are tablets and smart phones and moving towards the point where they're probably directly interfaced ... so, so I wonder if we can't—if we were to just say what is the, what is the razor's edge that we would like to say defines a riskier transaction. Um, is it being in premises that are not secured by the physical security of the organization? So for example, if a physician was the head of the department and had a secure line to his home, a dedicated, dedicated connection to his home, would that still be a riskier transaction because there's no guard from the organization outside the front door of his home.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Wes Rishel – Gartner, Inc.

Or are we looking for something, something different in this second bullet?

Deven McGraw – Center for Democracy & Technology – Director

I don't, I, you know, the second bullet was really just making sure because we had had some physical proximity discussions previously, but there's a reason why there's a question mark on that one because I, you know I wasn't sure myself whether that was a distinction beyond the first category that, that, that was terribly meaningful.

Wes Rishel – Gartner, Inc.

Yeah. Okay. Well, I'm, I then agree with your concern. Particularly I think proximity as we normally think of it, where you have to be, hold your badge physically proximal to the, to the device doesn't doesn't mean so much when you can pick up the device and carry it around.

Deven McGraw – Center for Democracy & Technology – Director

Right. Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think it was a different kind of proximity. But, I wonder if the, the physical location of the device is covered in a sense by the decision of an institution to put that device on the internal network or not. In other words, you're not going to put, you know the difference between logging in from their inside their network versus outside their network is often going to be highly correlated with the physical location of those devices. That's why the internal network is considered less risky.

Wes Rishel – Gartner, Inc.

Yeah, it's ... if we postulate that the internal network is not one in which any part could be unsecured or have an unsecured wireless connection then that the internal network is completely covered by the first bullet. I don't know whether it's reasonable to accept that as an assumption or not. But ... –

David McCallie – Cerner Corporation – Vice President of Medical Informatics

It's highly correlated.

John Houston – University of Pittsburgh Medical Center – Vice President, Privacy & Info Security

Could I suggest maybe a different way, we're all, of looking at this. I mean, I think we're all hung up on sort of trying to get our arms around the idea of a l– a location and maybe we should we think about doing this by attributes of what makes something secure and not secure and those attributes may exist whether you're inside of a facility or you're sitting at a physician's home or it may not. But if you're, you know, different attributes that we could assign that ... to be or not be securing such that additional authentication's required maybe that solves the problem.

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

I think it has to do with whether the device is actually under the control of the organization, you know, because organizations will push security features to devices, you know, to wireless devices, it may be, may be everywhere, but if it's like a bring your own device kind of thing then, you know, yeah, I would, I would require two factor authentication. It–it sort of, it, you know, we all know how conformance and compliance driven the health care industry is, it's almost like if it's outside the compliance control of the organization.

John Houston – University of Pittsburgh Medical Center – Vice President, Privacy & Info Security

Well that, that could be an attribute, to my –

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

Yeah, yeah. I agree. Yeah.

Deven McGraw – Center for Democracy & Technology – Director

I mean, I think we–I think generally what we're doing here is to sort of just create further examples –

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

Yeah.

Deven McGraw – Center for Democracy & Technology – Director

... of essentially this sub-bullet, sub, first dash under bullet two. It's to say, you know being, you know it's not part of the organization secured network, it's not a recognized IP address, it's outside of the compliance zone of the organization, you know then further clarifying what we mean by—by remote basically.

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

Yeah. Yeah. It's not supposed to be exhaustive, going back to ... comment, yeah.

Deven McGraw – Center for Democracy & Technology – Director

I mean I—you know I think folks can understand that. But let me, and, and that kind of a recommendation is one that is that communicates well policy wise in terms of sort of you know being, being as clear as we can be about the circumstances under which we think there ought to be multi-factor authentication, but also it doesn't have the precision that probably would be required for, say, a certification requirement. Is—is this something that we think is part of certification or is this better done through, through policy levers like meaningful use or NwHIN governance? You know, one of the things that I struggled with in thinking through that question is you know, we're not telling people they have to have a one size fits all multi-factor authentication solution where there's, there, even within the, the what's recognized under the NIST documents there are options that could be pursued.

Wes Rishel – Gartner, Inc.

I thought maybe what we were doing here was to inform Meaningful Use Stage 3? Is that -?

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Ask your question again, Deven.

Wes Rishel – Gartner, Inc.

Yeah. It sounded like you were saying ... question.

Deven McGraw – Center for Democracy & Technology – Director

Well, well, I'm sort of thinking through, we often get asked as, when my Tiger, when I present the Tiger team recommendations is if we have a specific direction in terms of the policy tool to be used to implement this. And so, one, one of the potential questions on the table is, is this a potential certification requirement or is this better done through more policy oriented tools like, you know, either a meaningful use objective or a governance condition, um for NwHIN.

Wes Rishel – Gartner, Inc.

I see. I think it goes directly to the issue that one of the speakers raised which is that they're looking for some support in the data about the relative merit of security of knowing who is, is behind the keyboard or the web screen, and the, the risk to patients of, of, of not having access to information. I think that whether some policy levers that could be used one of them is not certification of an EHR because generally all EHR's can be certified to, to do, you know, 14 level authentication if you want it. It's a question of what are the practices in use, well maybe only 13. But it could be a statement as part of a meaningful use conformance requirement for Meaningful Use version 3. It could be, it might, ... I think that the, the other options we have are like HIPAA which are not really sort of amenable to direct action by the ONC.

Deven McGraw – Center for Democracy & Technology – Director

Right, right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I would tend–this is David, I would tend to agree with Wes that certification is probably not a very meaningful way to enforce this because I'm pretty sure most people can demonstrate that they can support two-factor.

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

Well, I think, I think there's two, this is Dixie there's the ability to do two factor authentication and that should be a certification criterion, but, but the whole, the whole question of whether you actually require two factor authentication is an operational question that should be either meaningful use or HIPAA.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

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

But, but we do need it, you know, the capability as part of certification.

Wes Rishel – Gartner, Inc.

Well, I, I guess I'd just keep in mind that certification happens on a very strict budget in terms of the time spent evaluating an EHR product.

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

Yeah, but I can't imagine requiring people to use two factor authentication and then not having the EHR prod–product capable of doing it. Uh, people would have a fit about it.

Deven McGraw - Center for Democracy & Technology - Direct Chief Technology Officer

So, so, so here's an option that gets some of us off the hook but not all of us off the hook, which is, which is for us to be clear about the policy recommendation which we're, we-we've got, and then, you know, decisions about whether this would be part of certification or not. Do those really belong in, in, in your workgroup, Dixie, yours and Walter's?

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

Yes. We talked about it before, in fact, we discussed it with respect to the DEA requirement in Stage 2. But the requirement, we decided to postpone the requirement because DEA was still refining their recommendations.

Deven McGraw - Center for Democracy & Technology - Direct Chief Technology Officer

Right.

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

That's what we were told anyway.

Deven McGraw - Center for Democracy & Technology - Direct Chief Technology Officer

Yeah, all right, so, but if, but, I mean, first we have to get this policy recommendation to the Policy Committee, right?

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

Yeah. Yeah I agree with you it's more on the technology side, yeah.

Deven McGraw – Center for Democracy & Technology – Director

Okay, so, so I'm realizing that it's 3:27, so we're sort of quickly reaching the end of our meeting time and we haven't opened up for public comment yet. So what I'm going to do is I—I took really good notes about our conversation and I'm going to pass them around by email. But I think we did land on, you know more multi-factor authentication for the, for access to for user access to health information when, when, when it is coming from remotely, with definition of remote to include traveling across the network, any part of which is or could be unsecured such as an open internet or unsecured wireless connection when it's outside of an organization's secure network when it's not a recognized IP address for the organization, are examples of remote access circumstances. Does that roughly sound about right but to be wordsmithed better in writing for you all to look at?

Wes Rishel – Gartner, Inc.

Yes.

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

Yes.

Deven McGraw – Center for Democracy & Technology – Director

Oh.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Hey, hey, Deven, should we make an open-ended comment, though, that we, we will continue to monitor this as technology improves?

Deven McGraw – Center for Democracy & Technology – Director

Absolutely.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

So I think it might be good to say, we understand this is going to go somewhere, we're just not quite ready for it yet or not, or the industry isn't, but we're going to need to be mindful of that.

Deven McGraw – Center for Democracy & Technology – Director

Right. Right. I mean I think we can even mention that, you know, at least two of the examples were ... exploring it for internal use too ..., but since they were only in the exploration stage and had long ago implemented remote access this is the right first step to take.

Judy Faulkner – Epic Systems – Founder

And, Deven, can you give some thought, I haven't thought it all through, but could you give some thought to whether the second bullet becomes unnecessary –

Deven McGraw – Center for Democracy & Technology – Director

Oh it is. It's being removed.

Judy Faulkner – Epic Systems – Founder

Okay.

Deven McGraw – Center for Democracy & Technology – Director

Yep. Yes, Judy. Sorry I should have been more clear about that. We're really sort of focusing on–

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

You mean the second sub-bullet, right?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes.

Deven McGraw – Center for Democracy & Technology – Director

Yeah. Yeah. And I need to, I need to revise that first full bullet too per Wes' comment so it doesn't make it look like we're talking about HIE's specifically.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Right.

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

And to add authentication.

Deven McGraw – Center for Democracy & Technology – Director

Exactly. All right, folks, terrific call. MacKenzie, I know we're late.

MacKenzie Robertson – Office of the National Coordinator

No, that's fine. Operator, could you open the lines for public comment?

Public Comment

Operator

Yes. If you are on the phone and would like to make a public comment, please press *1 at this time. If you are listening via your computer speakers you may dial 1-877-705-2976 and press *1 to be placed in the comment queue. We do not have any comments at this time. We do not have any comments at this time.

John Houston – University of Pittsburgh Medical Center – Vice President, Privacy & Info Security

Yeah, Deven, you ended on time anyways.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, but I was cutting it close. Thanks, everyone.

John Houston – University of Pittsburgh Medical Center – Vice President, Privacy & Info Security

Thank you.

MacKenzie Robertson – Office of the National Coordinator

Thanks, everybody.

John Houston – University of Pittsburgh Medical Center – Vice President, Privacy & Info Security

Bye.

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

Bye.