

Privacy and Security Tiger Team
Draft Transcript
February 14, 2011

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director

Good afternoon, everybody and welcome to the Privacy and Security Tiger Team. This is a Federal Advisory Committee. There will be opportunity at the end of the call for the public to make comment. A reminder to Workgroup members to please identify yourselves when speaking.

Let me do a roll call. Devin McGraw?

Deven McGraw – Center for Democracy & Technology – Director

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Paul Egerman?

Paul Egerman – Software Entrepreneur

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Latanya Sweeney? Gail Harrow? Carol Diamond?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Carl Dvorak?

Carl Dvorak – Epic Systems – EVP

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

David McCallie, he is here.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Neil Calman? David Lansky? Dixie Baker couldn't make it. Micky Tripathi? Rachel Block? Alice Brown for Christine Bechtel?

Alice Brown – National Partnership for Women & Families – Director HTP

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

John Houston?

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

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Wes Rishel? Leslie Francis?

Leslie Francis – NCVHS – Co-Chair

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Adam Greene?

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Lisa Tutterow?

Lisa Tutterow – Office of the National Coordinator – popHealth Principal

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Joy Pritts is joining a little late. Did I leave anybody off? Okay, I'll turn it over to Deven.

Deven McGraw – Center for Democracy & Technology – Director

Thank you, Judy. Thanks for members of the Tiger Team who were able to make our call today. I think we have a lot of members who are traveling today in order to make the PCAST Workgroup Joint Policy and Standards Committee hearing tomorrow, so thanks to those of you who were able to make the time today and thanks also to members of the public who are listening in. We will have time at the end of the call, as per usual, to take public comment on anything we discuss today.

What we're going to talk about today is user authentication and we spent a little bit of time beginning this topic on our last call, but didn't really have a lot of time to deal with this issue. We do hope to be able to finish recommendations, not on today's call, but by our last call in February, which I think is a week from Friday. But, acknowledging that we are missing some members of the Tiger Team today who actually do have some expertise on some of these issues, Paul and I will be taking some time in between calls to circle back to them on any of the discussions that we have today. So that we are able to try to wrap this particular topic up by the end of the month, so that we can move on to patient identification and authentication and patient access issues in the month of March.

The other thing that I want to add is that on our last call we spent a fair amount of time soliciting your input on a document that MITRE prepared for us that looks at the PCAST recommendations and the Tiger Team recommendations in various categories where we've sort of covered some of the same issues. The chart compares sort of what we've said versus what the PCAST worker has said and we had solicited that for feedback. We got some great feedback both on our call as well as some offline and we were able to forward that document to the PCAST Workgroup.

I'll ask Judy Sparrow, I cc'd you on the e-mail that I sent to Dr. Stead and to Paul Eggerman. Would you mind, when we're done with this call circulating that to the Tiger Team and then I assume it would be up on the blog?

Judy Sparrow – Office of the National Coordinator – Executive Director

Right. I'll do that.

Deven McGraw – Center for Democracy & Technology – Director

Okay. Great, terrific. So, with that I will pause and see if Paul has anything to add before we jump into the meat of the discussion or if anybody has any questions.

Paul Egerman – Software Entrepreneur

Just excellent summary and I'm eager to talk about user authentication.

Deven McGraw – Center for Democracy & Technology – Director

All right. Then we'll move to discuss what's the objective of our discussion today and that is to determine whether the Tiger Team should consider any policy recommendations regarding authentication of user's accessing electronic health information and when we use the term users, we're talking about providers, clinicians, and staff within a practice or an entity. We are reserving users as meaning patients for March, as we mentioned before.

So, again, we're focusing on authentication of users to an EHR system; not patients, but, again, providers. The order of the discussion is to consider some different scenarios where setting policies on a level of assurance. For example, for user authentication, some use cases that we had discussed on our first call that might be relevant and that includes remote use—use that is not remote, necessarily, but uses a mobile device—and then users who are within their organization's network. This is one where when we get to it, we'll remind everybody what the Tiger Team had said previously on this issue and kind of road test that given the conclusions that we draw with respect to authentication of remote users and users who are using mobile devices to see if that recommendation still holds, if that's still the one that we want to promote.

With that, I think we should move into the remote use case and I'll let Paul take it away.

Paul Egerman – Software Entrepreneur

Great. Thanks, Deven. What you see on slide four is sort of an attempt to define what is meant by remote use and it says here authentication of users who remotely access EHRs via external networks such as the Internet. So, you've got this very interesting slide presentation where you have these three stick figures and it's hard for me to tell. It looks like they have the letter H on them; I think that stands for human.

Deven McGraw – Center for Democracy & Technology – Director

I was wondering that myself.

Paul Egerman – Software Entrepreneur

It's either Human or Harvard; I'm not sure which. But I think the indication is it's a human being and it shows in this diagram that they could be using a laptop, a workstation or a Smartphone, although we're probably talking about the remote the mobile devices later and most likely the Internet, but what I call a public network. Then on the right you see, there's a database and application and I think the purpose of this slide is to suggest there's actually a number of different technologies and vehicles. There's probably more than the three listed here. There could be a VPN, there could be a Web server, something called a proxy that facilitates this connection. But, basically we're talking about people predominantly under remote use they're probably working at what it calls workstations. Some people call them computer terminals or video terminals or laptops.

On slide five, it's sort of re-emphasizing this point with three use cases. First use case is a user accessing an EHR system from home using a laptop. The second one is a user accessing the EHR system from an airport using a portable device, a laptop or I suppose it could be some other device also. The third one that's interesting is it says user accessing software as a service system. In other words, a system that's hosted in the cloud as it were from a medical office, or it could be a hospital, but using a workstation via Web browser. In all these cases, the user is communicating the EHR System over the Internet or sometimes called the public network.

Before I go on, let me pause and see if people have any reaction to this sort of concept of remote access or access over the public networks.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

One consideration that I think is analogous, another notion of remoteness is whether there is physical security associated with the location that you're accessing from or a physical arrangement whereby your right to access that terminal is restricted in some way. So, the difference is walking to the nursing station and sitting down and logging in versus being in the airport using the exact same software to log in. In one case there's physical security and recognition of people around you. In the other case you're completely anonymous and that might be a distinction that's worth tracking.

Paul Egerman – Software Entrepreneur

I agree it's a distinction, but let me just point out, if you look at use case three, software as a service, you could have physical security, but you could still be accessing this system over the Internet and that could be a device in a hospital, for example.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, that was kind of my point is that it may be hard to tell just by virtue of whether you went "over the Internet" as to whether you are in a secured location or not.

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

If I might add to that, I think probably the more meaningful distinction is not necessarily where you're at, but often one is what is that workstation? Is that a workstation that is managed by the entity for whom you're access the data or is it a public device or a device that is actually owned by the employee? The reason why I make that distinction is twofold; one is that often you have less control over or no control over the device if it is not managed by that entity. Secondly, depending on how you provide the EHR access if there's a possibility that data gets downloaded to that device, again, if it is or is not within the control of the entity you may have other issues associated with loss of control over data. So, I think that's, in my experience, a more important distinction to discuss.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I agree with that, although I think even a managed device can be mobile. I have a managed laptop that I access from the airport and from home all the time.

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

I'm not denying that. My point is that when I have a managed device I can impose standards and other things that will provide a layer of security. I still have to worry about the transport and the like, but when you have no control whatsoever over the device and what might be on that machine, whether it be malicious software or otherwise or possibly the information gets downloaded and is lost because of somebody else's device I think is also incredibly meaningful.

Paul Egerman – Software Entrepreneur

These are good comments. Yes, go ahead, Carol.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

I'm wondering what problem we're trying to solve here in this discussion. Because while I appreciate devices have different levels of security the man at the edge attack, if you will, isn't there a set of policies that we get to first, which is how do you provide credentials to a legitimate user and how do you enforce those credentials or maybe we're done with that?

Paul Egerman – Software Entrepreneur

Well, we're raising a lot of the issues; to do my best to respond to your question, Carol, what is the problem that we're trying to solve? It's a very important question. What we're trying to solve is a very narrow problem. It's user authentication and the use cases that are described here are actually the ones that ONC is most concerned about right now. So it's really what, if anything, should the Tiger Team say about user authentication and I'm listening to these comments about whether or not you have physical control over the device or something called a managed device and to try to frame the discussion my suggestion would be well. Let's start with what I would call the worst case or the most challenging case.

Let's assume that there's no access to the device. If it's a physician's home laptop or computer or we're talking about a computer that's located at a hotel in the business services office that you can use and that somebody wants to log on with a browser because they need to do something while they're traveling. What I like to do is start with that as a remote use case and discuss just the very narrow issue of what level of user authentication are we going to require for that, if any.

We could decide that we don't want to address that issue, but that's the problem that we're trying to solve. The level is relative to the four list levels that we discussed before.

Deven McGraw – Center for Democracy & Technology – Director

In response to Carol's question I think it's important to sort of note some of the backdrop against which even the discussion as you framed it is occurring, Paul, which is in the sort of National Health Information Network universe there's certainly the universe of meaningful users. The HIPAA security rule, and we do have some background slides on this to remind folks already it does require that you have a process in place for identifying users to a system and that you be able to verify that the person seeking access to electronic PHI is the one claimed.

But the rule does not mandate specific implementation framework, nor does it specify authentication options or assurance levels or any types of verification. So I think what we're looking for, assuming a policy backdrop of already requiring processes to identify and authenticate users, are we as a policy committee and we as a Tiger Team advising the Committee going to suggest some more specificity on top of that with respect to certain use cases or even overall.

We're sort of piecing through these discussions on sort of more use case basis, in part because we had initially said as a Tiger Team that how institutions authenticate individual users of their EHR Systems internally was not something that we necessarily wanted to weigh in on in terms of creating additional policy beyond what the law already requires. Although we're going to have a chance to reassess that, but that's the overarching context of the discussion, you know, acknowledging providers, institutions are already required to have in place basic processes for identification and authentication; should there be some more specificity layered on top of that.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

So, that's very helpful, Deven. I think that based on the use cases and the context of our work the question is if there is a need for providers to participate in the NHIN or whatever the network, whatever the term is today and the network that we're talking about, should there be an evenness in the policy to authenticate them? In other words—

Paul Egerman – Software Entrepreneur

Carol?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

What is that?

Deven McGraw – Center for Democracy & Technology – Director

I don't know; that was very strange.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

That was very strange. Anyway, I don't know what that was. I was just saying that inasmuch as a level of assurance and trust is required across the network that is very different than the level of trust that's required maybe inside of the hospital where there are other protections in place. I do think that's the most paramount question, before we even get to once you get those credentials, how do they necessarily apply differently based on whatever device you're using, which is I think a different class of problems and a different set of issues.

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Is the output at some point of our process something that takes into account the tradeoffs between convenience and high level of assurance and we're speculating with constraints that could help guide people what those tradeoffs should be?

Paul Egerman – Software Entrepreneur

The likely outcome, the straw man that we're going to present is simple. It's going to be two-factor authentication, the NIST Level II.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And are we going to debate whether it's two-factor in some settings, but more than that in other settings?

Paul Egerman – Software Entrepreneur

Right, because the challenge there is going to be when you do something like that, the federal government says that the intention is that's like a four minimum. Sometimes, though, the minimum becomes the maximum because exactly as you just said, whenever you do anything with security—and I shouldn't say this definitively like I necessarily know what I'm talking about—but there's a trade-off, right, there's a trade-off between cost and usability and all of those things with the level of security that you get. Certainly, technology can help minimize some of those costs and can also make it a little bit more convenient to do whatever you're trying to do, but it's still that trade-off.

So the issue there is when we think about it do we want to set the minimum standard. There are some benefits for doing that because it raises everybody up to the minimum, but there might be some disadvantages to doing that and there might be some ways to address that, whether it's a standard or a best practice or a discussion document, there are a lot of issues. But that's sort of like the direction that we're going and so having said all that, maybe what I'll do is just race to the slide that says that because what is on the next slide, this is something that I think people instinctively know is when you're remote you're creating other potential vulnerabilities. If your credentials or tokens or other information is straggling over remote locations, there are vulnerabilities, exactly as John Houston I think was saying, you know the laptop that's owned by a clinician might not have the same security controls on it that other devices that the hospital or the medical office have and there's less physical access controls.

So, all of that is correct and then here's the guts of the discussion. The question is should the Tiger Team make a recommendation on the level of authentication required during these remote access use cases and the straw man answer to put forward exactly as a straw man to do the discussion is yes, we'll do two-factor authentication. The comments that are made there, one of them is because there's remote users, there's additional potential vulnerability and the other one is also just an observation the VA requires two-factor authentication for remote access to its EHR so that's sort of a data point.

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

Paul, do you really want to discuss this now or do you want to go through the rest of your presentation?

Paul Egerman – Software Entrepreneur

No, let's do it now. This is the guts of the issue.

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

Then I do have an opinion about that then. Having been part of a large organization that had a two-factor authentication solution and then went to something a little bit less that was sort of like a banking style, I don't know if I'd call it a one-and-a-half factor or, I don't know how best to describe it.

Paul Egerman – Software Entrepreneur

Could you explain what a one-and-a-half factor is?

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

Well, typically what it is if anybody does online banking it is—an applet is downloaded to the device that involves putting an image or selecting an image that the user recognizes as well as some type of pass phrase. What it is intended to do is it's intended to verify that the user is who they purport to be, or at least allow the user to verify also that they're not being directed to a site that is other than the one they think they're going to. So, you look at what happens in a banking environment if you bank using Bank of America and you go to their Website and it's actually a phishing site. Rather than your image being displayed on your device it will end up showing up is there will be no image, so you'll recognize you're not logging into the site you think you're logging into.

Paul Egerman – Software Entrepreneur

Right. Although another way you could look at that, what you just said, is you could say you're doing two-factor authentication, but for one of the factors you possibly chose something that is not on the NIST list. And so that would be one way you could do this, you can say we're going to do two-factor authentication, but we're going to define some expansion to some of these factors.

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

But the classic two-factor is something you have and that's why the RSA fobs, that's something you have and we've gone away from that because of cost and because of burden.

Paul Egerman – Software Entrepreneur

So, what you're doing is basically two things you know.

Deven McGraw – Center for Democracy & Technology – Director

So we do have a definition slide that MITRE prepared for us, which is on slide 16, which has two-factor authentication defined as requiring the possession of two tokens. Then, of course, what those tokens are it's my understanding that it doesn't necessarily have to be a hard token, like a Smartcard or something that is innate, like a biometric, but could be a password and a question. I think we have some MITRE folks on the call to help us through this.

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

That would be very helpful because I think if we go down that route, that is far less burdensome from the two-factor authentication schemes that some people think of when they think of two-factor authentication.

Deven McGraw – Center for Democracy & Technology – Director

Yes, I think the basic idea is something beyond just ID and password.

Paul Egerman – Software Entrepreneur

That's right. To me, what Deven said is correct from the MITRE briefing, the sense I had—and somebody needs to correct me if I've got this wrong—was you could have two factors that are both something you know. So his could be like one of those things where it says, "What's your grandfather's middle name?" and so that's something that you know, in addition to knowing your user name/password.

M

What the banks frequently do is take into account whether you had used this device before and/or have come from this IP address, so the challenge questions are not there every single time. They're there in appropriate circumstances.

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

Sure, and they've downloaded an applet to a device so that it recognizes that device has been previously used.

Deven McGraw – Center for Democracy & Technology – Director

Right, but that would be a token as well.

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

That would become a token, yes, you're right, Deven, you are correct.

M

They usually use a browser cookie for that, at least Bank of America does. They don't have an applet.

Paul Egerman – Software Entrepreneur

Yes, it's the same thing. I would consider that a token if you've authenticated yourself on that device once and they put something on the device.

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

A lot of them do, that's the token where some of them do put a token on the device.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Paul, is the correct way to frame the question and answer in terms of factors or in terms of levels of assurance? Because it seemed like the NIST document groups things by level of assurance and then for particular level of assurance, they say, for example, two-factor with hardware token, etc. I think the federal bridge document is also based on level of assurance rather than specific declaration of one or two or three factors.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

I'd also caution on that that you could have a single factor system that's much more reliable than a two-factor. I mean two-factor could be two things you know, but both readily available on Facebook, for example, versus a very strong password or a biometric as the single factor. But it's important to keep in mind two is not always better than one in this case.

Paul Egerman – Software Entrepreneur

So, what I'm trying to understand, Adam, from your comments is that an argument that says that you agree with David's statement that we should just base it on level of assurance?

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

Either that or spell out two-factor or single-factor a little bit more than just generically single-factor/two-factor because is one factor is a two-digit number, for example, that's not much of a factor at all, so it's important to have I think some parameters around what the factors are.

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

I would agree with that. I think we could be expansive in that regard.

Paul Egerman – Software Entrepreneur

So, I'm a bit confused. So, the first issue I want to understand is should we be talking about two factors or should we be talking about level of assurance?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

The reason I bring that up is that we've had the Privacy and Security Subcommittee, Dixie's Subcommittee or Workgroup of the Standards Committee is wrestling with the standards around entity authentication and we had several presentations at our last meeting, one from the VA, one from Arien Malec describing the direct projects. All of these presentations keep coming back to the two documents, the NIST document and the Federal Bridge document, which go on for literally 50 pages defining how you can meet certain levels of assurance and they don't talk about factors per se. That's built into the discussions about levels of assurance. It just seems to me that's where they've landed and that work is really thoughtful work.

Paul Egerman – Software Entrepreneur

So do we want to land in the same place is the question I'm asking.

Deven McGraw – Center for Democracy & Technology – Director

I'm moving the slides to the NIST document. I think the level of assurance makes sense, although I have to say, looking at it—so now I'm on slide 20, which is the NIST E-Authentication Guidelines SB800-63. Certainly, I think just innately you want high confidence for access to health information across a network by a provider, but in terms of sort of what that means you move from sort of single factor to then multi-factor, which is more than just one. So it's either two or it's two plus then I think some flexibility within that to make some specific recommendations about authentication level. Am I heading in the right direction?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I mean I like the way that summarizes; it's multi-factor, but it's not necessarily saying that that's two. It could be one factor if it's in a physically secure place where you're using a device from a network location that you've used many times in the past with a random challenge. It could be three factor if you're coming in on a device that you've never come in on before or over a network IP address that they've never seen before. So, it's flexible, but it's more than a factor, more than a single factor.

Deven McGraw – Center for Democracy & Technology – Director

Right. So, it's at least two things.

Paul Egerman – Software Entrepreneur

So, where are we coming down? Do we want to say two-factor? Do we want to say two or more factors?

Deven McGraw – Center for Democracy & Technology – Director

I think where we're coming down is that we want to set an assurance level for authentication across a network of a Level 3, which under NIST Guidelines means more than single-factor authentication.

Paul Egerman – Software Entrepreneur

Okay. Do we have agreement on that? Does anybody disagree? That's terrific.

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

It sounds like Roy Nist has done a lot of the heavy lifting.

Deven McGraw – Center for Democracy & Technology – Director

Well, they have, but I think in making choices is between the sort of Level 2 or Level 3, that, obviously, has some implications for what the set of expectations are in the healthcare industry.

Paul Egerman – Software Entrepreneur

Okay. So, I'm going back to slide number seven and what I've seen as our questions, "Should the Tiger Team recommendations on the level of authentication require these remote access use cases?" and our answer is yes, but we want the NIST Level 3 level of assurance, which means more than one factor authentication.

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

Then, to the earlier point, we also want to make sure we are very clear as to how we define two-factor and examples would maybe be good.

Paul Egerman – Software Entrepreneur

And that's a good comment because I want to get, I'm sorry?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I interrupted, I'm sorry. I was just going to say to John's point the NIST document does have a lot of good examples in it.

Paul Egerman – Software Entrepreneur

That's correct. Well, we got to this point which we got to in an impressive amount of speed; one of the ways we got here, though, was we sort of took off the table some of the issues or the questions that you raised, David, and John raised. Well, what happens if the device is managed? In other words, what happens if it's a device physically located someplace within in the hospital? Or, what happens if it's a

laptop, but somehow it's managed by the IT Department and they put some token on it or something or certificate on it so they could know what it is?

Part of my answer to that is, well, perhaps under those circumstances, that counts as one of the factors. Or maybe a better way for me to put that is in the form of a question. To the extent that the access to the device is somehow restricted or the device is somehow managed or controlled by the IT department, can that count as one of the factors?

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

Would you mind if I made a couple of comments here because I think it would be important. I think that the issue is twofold. When you have an environment whereby remote access only allows the individual to view remotely information, you have a certain set of issues associated with that, versus an environment where the user might be able to download information to their own device, or artifacts of that information end up being on that remote device.

So, you have those two different environments and you have to handle them differently because, obviously, when you download information there is information that has artifacts that are on the device and you have to worry about whether somebody can get at it or whether you lose control over it if there's not encryption, things like that. Then the other issue is with the idea of devices like mobile devices, Smartphones, how much control do you have over that device? Like one of the things we require, is a remote device we won't allow anybody to access anything if it can't be remotely wiped.

Paul Egerman – Software Entrepreneur

Let me just say first, let's take the mobile devices off the discussion for a minute because we're going to come to them next.

W

But that's not an authentication problem.

Deven McGraw – Center for Democracy & Technology – Director

Yes, that's right, it's not.

Paul Egerman – Software Entrepreneur

The issue also I have to say is I challenge your discussion about whether data is downloaded to a device or not. The reason is, the way I look at it, if I can look up information on my laptop, well, I can always write down on a piece of paper what I see, I can take a photograph of it, I can take a screen shot of it; there's a lot of things I can do. But the issue here is; another way to look at this issue is this is sort of like, just like a lot of things we do, the authentication piece is not the complete security solution. This is like the welcome mat. This is like how are you going to get into the first door; there may be other doors you have to go through so you're going to see a lot of other access rules that come further down the pike that are based upon the role of the individual, what they're doing, what they're able to access and so on.

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

Paul, I do need to just say one thing, though. We find in our environment that there really are two different types of issues. Yes, we want to make sure that the appropriate individual be accessing the data. But when you're dealing with user devices and laptops, things like that, if the device gets stolen and there is data on that device and devices get stolen often, you have to make sure that somebody can get at that data and use it for some inappropriate purpose.

Paul Egerman – Software Entrepreneur

I understand that, John. I think that's a great issue. That's the whole issue related to, there's a lot of issues related to laptops and mobile devices and encryption as a result. But that's not quite the issue that we're addressing here. We're limiting ourselves to the user authentication issue, which is simply the ability to access the information at the most basic level. That's what we're focusing on right now.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, are you who you say you are?

Paul Egerman – Software Entrepreneur

Are you who you say you are?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

It's identity; it's not even authorization, it's authentication.

Paul Egerman – Software Entrepreneur

You're right, it's identity authentication. It's who you think it is, what is the minimum for authentication?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

But these two issues become really entangled to the point where you can't almost separate them when you make decisions about how much you have to have in place, in my mind.

Deven McGraw – Center for Democracy & Technology – Director

Well, you certainly can't in terms of an entire security plan and all of this stuff is inter-related, but if we couldn't find a way to sort of parse it out and chunk up the discussion we'd spin ourselves into circles.

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

Okay, I accept that, you're right.

Paul Egerman – Software Entrepreneur

So, Deven has done a great job of reminding us of this slide from the MITRE presentation. In terms of authentication there's who am I, that's the identity; there is how is that identity represented? There is how can I prove who I am, which is what we're really talking about right now. There's the other step as David correctly pointed out, which is authorization, what can I do? So, we're really at the authentication piece, which is how do I prove who I am? That's what we are talking about. There are a lot of other issues to talk about in terms of losing laptops, but this is very much our focus and we've made great progress by saying Level 3 NIST is the name of them, which means more than one-factor authentication.

The comment that I made is we took these devices off the discussion and I want to put some of them back in the discussion by suggesting at least under some circumstances you could consider possibly that one of the factors, if you're using a restricted device. Were you trying to say something, David?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

No, I was going to, but I didn't mean to interrupt you.

Paul Egerman – Software Entrepreneur

I'm done.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Okay, then I'll add my comment, which is the other thing that I think probably bears mentioning is some notion that a risk assessment has to be done within the notion of Level 3 and it's not a fixed combination of things; it may vary, depending upon the risk of the particular access, the identity being spoofed. That's the approach that HIPAA takes and I think that the burden is on the provider of an identity service to understand the risks and to make sure that the technology matches the risk. That may vary, depending upon whether the device is sitting at the nursing station or is a cell phone not under managed control, you know, those two extremes.

Deven McGraw – Center for Democracy & Technology – Director

So, David, I actually think you're bringing up—you're sort of teeing up the next set of discussions, which we had kind of chunked into sort of use cases of mobile devices used within an organization, since we've already sort of declared that we want sort of higher levels for access across a network remotely. Then we had sort of teed up a sort of internal use for the sort of desktop within the facility question, but I'm now wondering if that's the right way to divide this up. And that what we should do instead is sort of think

about whether we want to provide some more specificity to the considerations done in the risk assessment, of sort of what within Level 3 are some sort of acceptable choices for a given set of scenarios.

Am I interpreting what you said right? I mean, the risk analysis is already required. I think some of the hesitancy at sort of stopping there is that we have a lot of physician practices out there that don't have a lot of experience with doing risk assessments and for whom some guidance about where to land might be more helpful for larger institutions who are better resourced. There's a sort of higher set of expectations I think, but even there, you want to create some baselines for trust across the network where if you are going to be sharing data institutions to institution, there sort of a shared understanding and a shared set of expectations about what's being done here.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, and I think that the examples as guidance is perhaps a good idea. The thing you have to watch out for is the fact that the technology is always changing. Every six months there's a new approach to identity verification and you don't want to exclude something because you didn't mention it or to lock people into a technology that gets bypassed. I think that's why NIST took that approach to say there is no specific technology, but here are the things you need to think about.

W

But, you know, David, that's a really important point and it does speak to a possible recommendation to the federal government to be viewing the kind of R&D on these different modalities and methods and it's been the kind of R&D on these different modalities and methods in an ongoing way so that best practices do emerge.

I know back a handful of years ago when we looked at this issue in the common framework, everyone had assumed in-person authentication was the gold standard. Clearly, everything you read sort of said, yes, when you come to the office and I know who you are and I see your face and I give you credentials, that's a pretty surefire thing. We couldn't find any data on the outcomes or the results of in-person authentication versus knowledge-based or other methods and it does speak to, especially as we move more to knowledge-based systems and Web enabled systems, it just speaks to a need to have an ongoing research effort to understand the performance of these.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes, that's a good point and I agree that this is a rapidly evolving field. I mean in our own product offerings, just since last year we've introduced several new authentication mechanisms that are designed to just make it faster for the physician to walk up to a station and pick up a session that they suspended at another station by simply waving their badge at the screen. Just constantly changing technologies that you go through the risk assessment and say this is multi-factor and it meets the NIST step Level 3 definition, but the technology is going to be completely different in a year or two.

Paul Egerman – Software Entrepreneur

David, I'm trying to understand what you're suggesting. Are you suggesting that our recommendation be Level 3 NIST and something about risk assessment?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, I think Deven's point is a good one, that they're already required to do the risk assessment and maybe it's not necessary to repeat that. I guess the only thing I'm suggesting is that a recipe isn't going to be adequate. We can't specify the ingredients and say do it this way, you know, password must be six characters and change every six weeks.

Paul Egerman – Software Entrepreneur

David, now I understand. So, basically, if I'm hearing you right it's sort of a sense of it's not only can't we do that, it might be dangerous to do that because as technology changes we might be carving something in stone that is inappropriate. So, does that sort of suggest that we say NIST Level 3 and then we shrug our shoulders and say now we're done. I'm just trying to understand. Are you making a suggestion that

we shouldn't screw around with what it already says there. We shouldn't say this really counts as a factor and this one doesn't because that's what the whole NIST thing is and that's kind of a moving target. Is that a reasonable conclusion or an unreasonable conclusion?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think it might be reasonable to set that as a lower bar; I think that there are institutions, including the VA, if I recall from the discussion last week on this other conference call that their circumstances were that they require Level 4.

Deven McGraw – Center for Democracy & Technology – Director

Right, no, Level 3 would be the minimum.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah, exactly, we'd have to specify it as a minimum.

Deven McGraw – Center for Democracy & Technology – Director

But even then, I think we can also make some statements about, so Level 3 being the minimum, which requires more than a single factor. That entities already are required to do a risk assessment in terms of establishing what factors will be required for authentication, that there ought to be best practice guidance issued on a regular basis as to effective authentication technologies and methodologies. That HHS should be doing some research and dissemination of best practices as sort of similar to what we've been doing, similar to what we've said in our previous set of recommendations on patient matching. You know, in these fields where technology is constantly evolving, you know, better information about what works and what doesn't and some research as these things get deployed is certainly going to be helpful. I think it's particularly important on the guidance issue for the smaller practices, for whom security is not something that they know very well and who are probably going to be relying pretty heavily on their vendors for some assistance.

Paul Egerman – Software Entrepreneur

I think what you just said, Deven, sounds great. There's one little concern that I have when you talk about best practices around technology. I'm a little bit nervous only because security technology is a very competitive field and so I sort of have this picture, like, oh, geez, I'm a vendor and I've got some new security token that I think is fantastic. So the next step I've got to do is I've got to get myself in front of HHS so I get listed as a best practice. So, maybe best practice might be methodology, but may not necessarily be technologies, or at least to the extent it's technologies, it's not specific technologies. It's general things like biometrics, it's like a class of technologies.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Again, I think that NIST document does a nice job of reviewing those, kind of categorizing them as something you have, something you know, something you are and then giving examples, but it's not an exclusive list or an exhaustive list. So cameras on the PC that can recognize your face may make biometrics all of a sudden extremely cost effective, whereas they haven't been in the past; things that are just still cutting edge, but they will come out because the demand for convenience and security is a constant pressure.

Paul Egerman – Software Entrepreneur

So, again, to reiterate what I think I heard from you, Deven, was I heard four things, which is our recommendation is for Level 3, which means more than one single factor, at least more than one and that's a minimum. To perhaps make some comment to entities that are already required to do a risk assessment; that HHS should have best practices on security, maybe methodologies and number four is, this is an area for continued research. HHS should do continued research. Did I get that?

Deven McGraw – Center for Democracy & Technology – Director

I think you did.

Paul Egerman – Software Entrepreneur

Do we have a consensus on those four points?

Deven McGraw – Center for Democracy & Technology – Director

Yes.

Leslie Francis – NCVHS – Co-Chair

Paul, not a change; just a modification that the research doesn't necessarily have to be done by ONC, but it's NIST or whoever, but there should be an effort to support that.

Paul Egerman – Software Entrepreneur

Yes, and actually in my notes I wrote HHS.

Deven McGraw – Center for Democracy & Technology – Director

Right, but NIST isn't part of HHS and so there's a federal government role here.

Leslie Francis – NCVHS – Co-Chair

Yes, and I mean this is a challenge that is cross-sectoral. It's not a health authentication issue, right? I mean the research that's needed potentially could come from each of the sectors, financial services included, just using different modes.

Deven McGraw – Center for Democracy & Technology – Director

Yes, that's a really good point. We don't have to invent these special health solutions.

Leslie Francis – NCVHS – Co-Chair

And actually it's unlikely to work because people are people.

W

Leslie, that's very good. There are a lot of efficiencies in just going back and forth from different sectors.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And the banking industry, in particular, has worked very hard to figure some of these things out, because they, obviously, have a strong incentive to get it right and yet not to alienate their customers.

Deven McGraw – Center for Democracy & Technology – Director

Well, and there is the federal initiative, the National Strategy for Trusted Identity in Cyberspace that is not a product of HHS, but is a federal government initiative to create a national trusted identity system that will work over the Internet.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

The other, we're in such violent agreement here I wanted to upset the apple cart a little bit and just come back to one question that we passed over, which I think is probably not an issue with respect to providers. Maybe it's something that is more of an issue when it comes to patients and consumers, but part of the assurance level is the degree to which you do identity proofing when you issue the credential in the first place, when you assign the password or give them the token. In the consumer space, that's a big question, how much proofing. Although with providers in the DEA they have some very precise requirements over what it takes to get the adequate tokens to do electronic prescribing.

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

Let me just say, on the consumer side, David, great comment. That's what we will hopefully do in the month of March is we're going to attack that issue on the patient and consumer access issues, as it relates to patient portals and EHRs and all that, it's wonderful stuff. This discussion is limited to I call it EHR users because it may not necessarily be physicians or even clinicians.

Deven McGraw – Center for Democracy & Technology – Director

Right, it could be staff.

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

The reason to bring it up was to simply maybe say, and maybe this is just part of discussion, not a bullet point, but the assumption is that the staff will have been identity-proofed through existing procedures at the institution.

Paul Egerman – Software Entrepreneur

That's correct. There's a different issue, especially if you have a staff of five employees, but even if you have a staff of 3,000 or 10,000, it's a different issue than if you're dealing with 200 million people.

Deven McGraw – Center for Democracy & Technology – Director

That's right, and I'm almost thinking that it would be helpful to, in terms of framing these recommendations as we finalize them to really cite what is required under the security rules, so that people don't think we're missing something or starting from scratch. There is a baseline on which we're trying to build here.

Paul Egerman – Software Entrepreneur

So, now that we're in violent agreement on this—to pick up your expression, David, and also just remembering some of your other comments—and we do not seem to have any dirt to push under the next rug, that's a problem. But maybe we'll get that in a minute because the next thing we wanted to wrestle with is the mobile devices and are you going to take us through this, Deven?

Deven McGraw – Center for Democracy & Technology – Director

Well, but we sort of created these; I actually think that this next set of slides on mobile devices and then the two that follow that are about internal use, I might want to chunk them together a little bit.

Paul Egerman – Software Entrepreneur

I'd actually like to keep them separate.

Deven McGraw – Center for Democracy & Technology – Director

You want to keep them separate? Well, let me tell you what I'm; I just want to lay the framework for where we're headed. The set of recommendations that we just got consensus on were about access across a network or remote access. These next two are about access within an organization, so whether you're using a mobile device within an organization or you're using something that's not mobile, something that's fixed, like a hard drive or a laptop within an organization, that's certainly the way and MITRE helped us to frame this. I think the expectation was that if you're using a mobile device external to an organization remotely that that's sort of picked up by the remote use set of discussions that we've already had. That's why I was chunking them together.

Paul Egerman – Software Entrepreneur

Okay, if that's the case and that's the distinction I missed, I want to actually think a second about the mobile device and what we just said about Level 3 because I just want to ask, there's a lot of people using these things now. These things like iPods, iPads, all these number of screen oriented, Smartphones, BlackBerry has them. There are a lot of devices out there and people are using them. They get access to the Internet, they're getting lab results on them and the question, though, is does that Level 3 that we just said, does that work in a way that people are comfortable with so that people can use their iPods and iPads from home?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

To me, it's really a different question. Typically, users don't have different authentication policies based on different devices. There's a level of assurance for initial credentials and access and if IP address, for instance, or a device is part of the authentication construct, and I think somebody alluded to this before, there may be additional procedures in place to verify, re-verify or re-authenticate, so if that's the question, which banks do typically also, I think that's good. But I guess I'm just wondering; are you asking this because you believe that we have to come up with a different set of requirements completely for mobile access?

Paul Egerman – Software Entrepreneur

I am asking it because I just want to make sure that we've got this sort of—I don't know what the right word is. People use the word burgeoning or something, this sort of rapidly expanding use of mobile devices and people love them and I suspect, though, a fair amount of the state of the art is to use an iPhone and just type in a password. If I understand what you're saying, Carol, is as well, that's probably okay as long as you've got something about the device that represents the second factor, you know, like you've registered the phone number or the ID number or something and that's being checked as part of the process.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Yes, I guess I'm saying the issuance of your initial credentials should be irrespective of the device. You can't pretend to be a physician through some mechanism and get into the system. There should be a level of assurance initially for you to get those credentials and then how you use them on what device I think is the next level of question.

Deven McGraw – Center for Democracy & Technology – Director

Okay, Carol, explain what you mean by the how you use them part of your comment.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Well, typically, if there's a site where you've been authenticated—think of your bank this way—if there's a site where you've been authenticated, they go through some multi-step process initially to sort of give you access, they e-mail you something and then you have to log back in or whatever. Then you're in. And if you log in from that same device consistently, it's pretty seamless. If you try to log in from a different device because your IP address was part of how they knew it was you, they may put you through some new paces, but you still have to have the process that was in place when you got your initial credentials. In other words, you still need those credentials. So, you've got a circumstance of more than one factor being required, but based on the risk assessment, which are the tokens that authenticate you is going to differ based on the device you're using, but it still meets at least a Level 3.

Paul Egerman – Software Entrepreneur

Yes, I understand what Carol is saying, if I got it right, it's sort of like if I'm using an iPhone to get laboratory results, what my application does is ask me for a password and maybe the first time I use it, it's one of these things that it asks me for my father's middle name or something. I give that, but then if the application can identify that I've answered it correctly based on my phone number or based on some file that gets set somehow along the iPhone then subsequent accesses, I might need just a password because I've got basically possession of an authenticated device as my other factor and so that makes sense. If I hear Carol right, saying back what Carol said, let me see if I've got it right, is sort of like how you choose those factors, you know, you choose them that they're still factors, but they're convenient or reasonable for the device you're using.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

Yes, it's a next layer of questions, but the sort of making sure that I gave you the right credentials the first time and that I know that I gave them to the right person is a persistence policy.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I hate to keep talking about NIST, but the distinction that they make between Level 3 and Level 4 is that Level 4 requires a hard token; it can't be one of the soft factors that we've been talking about. So, I think one of the questions that we could address is are there circumstances that we could specify in sufficient precision so that people would know what they meant where we would say you have to go to one of those areas.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

And is mobile one of those areas.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And is mobile one of those would be exactly the question. I think the answer is going to be no, but I'm not sure.

Deven McGraw – Center for Democracy & Technology – Director

Can you remind me, David, what qualifies as a hard token?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

It would be something like a key fob that has a number on it that you have to type in or it could be a smart card that you swipe through the device.

Deven McGraw – Center for Democracy & Technology – Director

So, authenticating the device would not be sufficient?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

It's not sufficient to simply answer questions on the screen.

Paul Egerman – Software Entrepreneur

I think it's a good question, but, David, I like the fact that you asked the question, but I also liked your answer to it. It's like one of these things that's personal. I mean I look at my BlackBerry and I figure I'm willing to lug that around, it's not real heavy. But if I've got to lug that around and I've got to keep like one of these RSA keys and I've got to type in the number from the key into the BlackBerry somehow and a BlackBerry is a little bit easier than a keyboard, but if I've got one of these things that doesn't have a keyboard. It strikes me that that's the kind of thing that people are going to get very frustrated by.

Carl Dvorak – Epic Systems – EVP

I think we also have to respect that people often will lose them in tandem, if you really made the world a better place.

Paul Egerman – Software Entrepreneur

Well, adding to the thought about that, that's right, it makes sense, right, what you just said, Adam, makes a huge amount of sense. If I had to use both I would like tape them together—

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

That was Carl.

Paul Egerman – Software Entrepreneur

—one on back of the other so I'd lose them both at the same time. So that sort of undermines the concept of it.

Carl Dvorak – Epic Systems – EVP

Yes, I also wouldn't undervalue the utility of a strong password. It turns out to be the physical things often get lost together, but the password if you really do it from memory and that, obviously, means you're not changing it so frequently to have to write it down somewhere. But the value of that is good and although the computer science people will tell you that it can be broken, that's only really true if you don't have a throttle on how many attempts a person can have if you force it, a time between attempts and a maximum number of attempts. It turns out to be extraordinarily strong and I just worry that what I've seen in other countries they go so overboard on some of these things that people just shy away from using the computer in the first place and they fly blind rather than access information through a device simply because it's so inconvenient to attempt it.

Paul Egerman – Software Entrepreneur

And, Adam, those are great comments.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

That's Carl.

Carl Dvorak – Epic Systems – EVP

It's Carl, Paul.

Paul Egerman – Software Entrepreneur

We're going to get the passwords in a few minutes.

Leslie Francis – NCVHS – Co-Chair

Well, it does really point to the need for projective based... of these different methods. I think Adam raised the point earlier that a lot of these knowledge-based systems, which are presumed to be potentially stronger may not actually be because so much more data is available publicly.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program

It's exactly why it would be good to have some objective research done.

Paul Egerman – Software Entrepreneur

So, great discussion. Let's get back to slide eight, you were saying, Deven, that you wanted to combined this with the next one and I sort of screwed up by saying preferably not mobile devices. I think we discussed this; I'm satisfied with that issue, so let's get back to, unless people want to do something else, back to where we were on slide eight.

What were you saying, Deven?

Deven McGraw – Center for Democracy & Technology – Director

Well, I think that we don't have a different answer for slide eight than we do for, at least with respect to authentication. I mean there might be some other security issues raised by mobile devices, such as transport security, whether text messages can be sent securely and whether that's a good communication vehicle. But in terms of the authentication issue I'm not persuaded from the discussion we just had that there's any change to the basic set of recommendations that we've been coming to consensus on.

Carl Dvorak – Epic Systems – EVP

I agree with you, Deven. I think the notion of whether the keyboard is attached to the screen with screws and plastic versus not, is kind of an outdated notion. I they all should be treated the same whether it's a laptop, a Tablet or a Smartphone.

Paul Egerman – Software Entrepreneur

Also, was that you, Carl, that made the comment?

Carl Dvorak – Epic Systems – EVP

Yes.

Paul Egerman – Software Entrepreneur

I apologize for getting that wrong.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And, again, I think the NIST approach is not to be specific about those details, but rather the degree of certainty and you could come up with circumstances where you know you have to work harder to be certain, but the burden is to be certain, not to specify how hard you have to work.

Deven McGraw – Center for Democracy & Technology – Director

So, I think given that, then the other question that we had teed up, is given the set of policies and the minimum assurance level across a network are we still comfortable with saying that with respect to individual users who are accessing within an enterprise, sort of what the minimum level of assurance is, we wouldn't set that for internal access. Again, previously when we did provider entity authentication we were comfortable saying that individual institutions and provider organizations should develop and set their own policies with respect to internal identity and authentication, when it's not being done across a network. Does that still hold or now that we've sort of landed so comfortably on a minimal Level 3 and

acknowledging that physical location might be, the physical IP address of the work station might be a factor that sort of gets you over the single-factor and into multi-factor; do we want to sort of apply Level 3 across the board? I hope that made sense.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think the answer; I would answer yes, if I understood your question right.

Deven McGraw – Center for Democracy & Technology – Director

Yes, so in other words, our conception of what minimal Level 3 requires and the fact that there are still choices that need to be made with respect to what are the tokens that are required for authentication that Level 3 really ought to hold within an institution or practice.

Paul Egerman – Software Entrepreneur

Yes, and so just to be clear, if you do Level 3 within an institution, the way I'm understanding it, we are also saying physical presence at a device that's connected by a private network to a computer. In other words, not over a public network not over the Internet, that physical access at a device within the institution and a private network that that by itself counts as one factor. Is that right?

Deven McGraw – Center for Democracy & Technology – Director

I believe it is, so that then if you're requiring sort of password for entry.

Paul Egerman – Software Entrepreneur

So my response was, I guess I would agree with David. The only thing that gives me pause a little bit as I think about this is just the issue of the minimum and the maximum because I know there's a lot of institutions where the CIOs have done great work with security. They'll do things like they'll do card readers with the workers' ID cards so the ID card that might be necessary to get into the facility can also be used to somehow get into the computer system and they make you do that and they make you put in a password. I don't want to discourage that kind of stuff because that's good. So, that's just a comment. As long as we're not discouraging that, I'm okay with Level 3 for internal.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think that's pretty standard in most places.

Paul Egerman – Software Entrepreneur

When you say standard, David?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think it's pretty common practice to have that level of assurance, certainly in large institutions. I'm not sure about two man office practices, but many, I don't know what percentage, but many of our clients use the employee's badge as a token and have a reader; you tap the badge on the reader and put in a four number PIN and you're in.

Paul Egerman – Software Entrepreneur

Yes, my point is if we say Level 3 and if we say physical presence at a device that's connected by a private network counts as one factor, then are we saying to those institutions you don't have to do the badge anymore?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Oh, I see what you're saying.

Paul Egerman – Software Entrepreneur

I mean, are we setting a standard that's lower than common practice?

Deven McGraw – Center for Democracy & Technology – Director

Well, I don't think so, because you need more than one, so at a minimum you're going to have to have some sort of password or knowledge-based authorization to get in beyond the physical location of the device, because that would just be single-factor and that's not Level 3, right?

Paul Egerman – Software Entrepreneur

Yes, but what we're saying is common practice right now is physical presence at the device, presence of an ID card and the usage of a password.

Deven McGraw – Center for Democracy & Technology – Director

Well, no, I don't think the card is necessarily common practice.

Paul Egerman – Software Entrepreneur

I think David just said it was.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

It's increasingly common and the reason that it is is the convenience factor is that you don't have to type in your user name. You just have to PIN yourself in and so it's both more convenient and more secure, so, it unfortunately costs more, too, so not everyone does it, but it is increasingly common.

Carl Dvorak – Epic Systems – EVP

There's another common practice, though, with those cards and that is the card will challenge the user every so many log in attempts, so they'll go without a password or without a PIN number up to some reasonable number of times and then it will force them to put in a password again or to do another PIN. So that you get the convenience of it and I've also heard people now discussing the notion of differentiating between single patient record access versus capabilities to maybe download a file or something like that to compromise access to features that might compromise longer lists of patients. Versus being able to see a single patient record and people are looking at differentiating security for those two scenarios.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And the BEA requires a differentiation around the e-prescribing of controlled substances versus non-controlled substances.

Deven McGraw – Center for Democracy & Technology – Director

Right, which is all good. For institutions to head to requiring greater security is a good thing, but I guess the point that I was making, and not very well, before is that by requiring a minimum level of three, you certainly have institutions that can do more in their own interests and based on their own security risk analysis. But it's also a level that arguably a physician practice could meet that didn't use a card for its internal users.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

I'd recommend on Level 3 it may be helpful to have someone from NIST really talk about exactly what Level 3 means, because I'm not sure that some of the statements that have been made are entirely accurate with respect to what really is required for Level 3. This goes somewhat towards Paul, I think, with respect to whether a device authentication can count as one of the tokens. I'm not so sure about that, so it may be helpful to have someone opine on this.

Paul Egerman – Software Entrepreneur

I think that's great because—that's a great suggestion.

Deven McGraw – Center for Democracy & Technology – Director

Yes, I think it's a good suggestion, too, because even looking at the slide that we have from MITRE, this is just a snapshot of what's in those guidelines; they're much richer in content.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

Right, I'm reading it right now, the actual NIST guidance, and it talks about a minimum of two authentication factors is required, three kinds of tokens can be used, "soft cryptographic tokens," "hard cryptographic tokens" and "one-time password device tokens." So, it would probably be helpful to have someone explain exactly what that entails.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

That sounds right.

Deven McGraw – Center for Democracy & Technology – Director

Okay, we can do that. We will hold on our straw man of Level 3, but use our next call to get some clarity about what that is going to entail, particularly for small practices. I don't think what we're suggesting is going to be a major leap for most institutions and maybe for those that it is a leap, maybe it should be a leap, but when you're talking about the smaller organizations, I think we need to understand what the impact is going to be.

Paul Egerman – Software Entrepreneur

Deven, if I understand Adam right, it's not just the small organizations. Adam is saying—well maybe my comments about devices aren't quite right. So it would have an impact on what we said about mobile. It would have an impact on what we said about internal users, too. We need to clarify that. The issues is between Level 2 and Level 3, did we really make it all the way to Level 3 or did we actually end up in a gap between Level 2 and 3; it's more than one factor, but it's not quite what NIST considers two factors.

Deven McGraw – Center for Democracy & Technology – Director

Or multi-factor really. Level 3 is multi-factor.

Paul Egerman – Software Entrepreneur

Yes, so maybe we are at one and a half.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist

Yes, my concern is Level 3 is not just multi-factor; that's kind of a starting point, but Level 3 has particular requirements with respect to what factors can be used and I think that's where we're all a bit fuzzy.

Deven McGraw – Center for Democracy & Technology – Director

Lisa Tutterow from MITRE, is Jay on by any chance?

Lisa Tutterow – Office of the National Coordinator – popHealth Principal

Yes, we're here.

Deven McGraw – Center for Democracy & Technology – Director

Okay. I don't know if you want to opine on the discussion that we've just had on what NIST suggests for Level 3.

Jay Brennan – MITRE

Well—

Deven McGraw – Center for Democracy & Technology – Director

Is this Jay Brennan from MITRE?

Jay Brennan – MITRE

Yes, it's true that if you're going to take Level 3 hook, line and sinker, then you've got to do a whole bunch of other things, but I don't think you guys have to actually recommend; you can just say that the methods match NIST Level 3 without taking all the rest of the baggage with it. I think that's certainly possible. But it is a good caution to know that there's a lot more to Level 3 than just picking two factors. I don't have the words in front of me, but I think if I found the NIST document I would find out that the work station that you're at does not count as a factor. I think that's actually specifically prohibited in the wording, but I can't

recall exactly where it is. So, I think that's probably going to prove out to be a fact, that the work station that you're at does not count as one of the factors.

Joy Pritts – ONC – Chief Privacy Officer

I think I'm on the same page and it's that the factor has to be something other than the equipment that you're using to access the system.

Jay Brennan – MITRE

Yes.

Paul Egerman – Software Entrepreneur

So, I'm trying to understand these comments. So, we had this great sense of comfort about where we were related to mobile devices. Should we be uncomfortable now?

Deven McGraw – Center for Democracy & Technology – Director

Well, Paul, when you say with respect to mobile devices, are you talking about access across a network externally or internally?

Paul Egerman – Software Entrepreneur

External.

Deven McGraw – Center for Democracy & Technology – Director

Okay, so maybe we're not necessarily comfortable with where we are externally beyond just the mobile device issue.

Paul Egerman – Software Entrepreneur

Yes. So, our next step is we're going to get somebody from NIST or, Jay, we're going to research this a little bit? Is that our next step, what are going to do?

Joy Pritts – ONC – Chief Privacy Officer

I can get somebody from NIST to give us some more information if you want.

Deven McGraw – Center for Democracy & Technology – Director

Yes, I think that's helpful because I think we have made some assumptions at arriving comfortably at sort of Level 3 across the board that we're going to need to pressure test, given the sort of comments of the last 15 minutes.

Joy Pritts – ONC – Chief Privacy Officer

Okay. So, do you want me to line him up to talk to the entire group at the next call?

Deven McGraw – Center for Democracy & Technology – Director

Well, and I think initially as we sort of prepare for the next call because we really wanted to finish this by the next call; I think we might need to have that conversation initially on our planning call.

Joy Pritts – ONC – Chief Privacy Officer

Okay. Do you know when that is offhand, when our next planning call is, because I'm trying to put this on my calendar.

Deven McGraw – Center for Democracy & Technology – Director

Unfortunately, I think we're going to have to figure that out because it lands during HIMS. So, we might have to find some time on the schedule for it maybe this week, but we should do that offline. In the interim we will also gather some of that background material.

Joy Pritts – ONC – Chief Privacy Officer

Lisa, would you mind trying to schedule that?

Lisa Tutterow – Office of the National Coordinator – popHealth Principal

Of course.

Joy Pritts – ONC – Chief Privacy Officer

That would be awesome.

Deven McGraw – Center for Democracy & Technology – Director

So, here's what we'll do, folks. Again, given that we made some assumptions about what is required in terms of authentication for Level 3 we will be able to dig into that a little bit more so that we can have a final call a week from Friday to just finalize this.

Joy Pritts – ONC – Chief Privacy Officer

Is Dixie on the call today?

Paul Egerman – Software Entrepreneur

No, she's not. She's traveling.

Joy Pritts – ONC – Chief Privacy Officer

Deborah is in a meeting, too, because I know that there were issues on this with respect to DEA authentication in that it wasn't a—and I think we've heard this from them before, which is it wasn't a—precise match of what the requirements of the NIST level were and what we thought we could do, even for DEA authentication. Do you remember that conversation at all? Just vaguely, that's all I remember. I remembered enough to know that we had it, but not enough to know what the details were.

Deven McGraw – Center for Democracy & Technology – Director

Yes, okay. That's about my vague recollection as well. All right. Well, I'm not sure that there's much else we can do today, Paul.

Paul Egerman – Software Entrepreneur

Well, I think it was a good discussion. We've advanced where we are.

Deven McGraw – Center for Democracy & Technology – Director

I think we know where we want to land. We just need to understand what the implications of that are.

Paul Egerman – Software Entrepreneur

Well, that's right because the way I look at it, let's get more information from NIST. We certainly know where we want to land. NIST might tell us that we landed where we want to be and if we didn't land where we want to be, then I think we might get some ideas as to how to get there. So, I think this makes sense. The only other issues that we had keyed up on our slides were sort of like questions. One question is do we want to talk about what constitutes authentication and let's wait to hear from NIST about that, in terms of what's acceptable factors. If NIST has got that down right, then we don't need to do anything.

The next slide, slide 13 is interesting, should we be also entering this whole are of password use, you know, password strength and the number of times a password is used.

Joy Pritts – ONC – Chief Privacy Officer

That seems a little down in the weeds as a policy group.

Paul Egerman – Software Entrepreneur

I agree.

Deven McGraw – Center for Democracy & Technology – Director

Feels like a good guidance topic, though.

Paul Egerman – Software Entrepreneur

Yes, it could be a good guidance topic, but also I don't think a policy committee necessarily wants to be the one that tells anybody how to do it. That's like Standards Committee or somebody should.

Joy Pritts – ONC – Chief Privacy Officer

Yeah, that seems to me like something you can say. We need, ask for the specifics of what would be good. Maybe somebody should be issuing—like us—or OCR issuing guidance on it for best practices.

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

And if we go to NIST levels of assurance that incorporates, I think, some password strength requirements.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And it's not intuitive the common practice of making people change their password every month is a bad way to do it, so sometimes teaching people a little bit about saying password practices is a real benefit to everyone.

Deven McGraw – Center for Democracy & Technology – Director

I have to say, there's some stuff, I think David is exactly right, there's some stuff that's not intuitive in there, but it's very easy to adopt for an individual user.

Joy Pritts – ONC – Chief Privacy Officer

So, it's the usability factor on top of the security factor, because if they don't use it right, they aren't going to be using it.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And just the fact that sometimes things which seem highly secure turn out in practice to not be secure and like the frequently changing password everyone solves that problem by writing it down.

Joy Pritts – ONC – Chief Privacy Officer

Right. So, it's not usable, so they write it down, they stick it on the computer and now what kind of security do you have? None.

Deven McGraw – Center for Democracy & Technology – Director

Right. Or if they don't stick it in the computer it goes in the Contacts database under password.

Joy Pritts – ONC – Chief Privacy Officer

I hadn't thought of that one yet.

Paul Egerman – Software Entrepreneur

I think, Deven, I think we've got a good discussion going to today. We know where we want to land.

Deven McGraw – Center for Democracy & Technology – Director

It always helps to be able to figure out what we need to nail down, by the next call.

Paul Egerman – Software Entrepreneur

And I think we've got that, although maybe we'll be lucky and in the public comment phase.

Deven McGraw – Center for Democracy & Technology – Director

We'll be enlightened.

Paul Egerman – Software Entrepreneur

Will be able to enlighten us.

Deven McGraw – Center for Democracy & Technology – Director

Yes. So, Judy, can we go to public comments?

Judy Sparrow – Office of the National Coordinator – Executive Director

Sure. Operator, can you check and see if anybody wishes to make a comment?

Operator

You do not have any comments at this time.

Judy Sparrow – Office of the National Coordinator – Executive Director

Okay, thank you. Thank you, Deven and Paul.

Paul Egerman – Software Entrepreneur

Yes, thank you very much.

Deven McGraw – Center for Democracy & Technology – Director

Thanks, everyone. For those who are coming in person tomorrow, see you then. Stay tuned and safe travels.

Public Comment Received During the Meeting

1. If authentication factors are associated with the mobile device then you could as well use zero factors. My mobile saves passwords and if another factor is set on the phone so when it is stolen everything will be in the possession of the holder of the phone.
2. If you use something like a cookie or app on the device, then you are not meeting the requirement that the token be separate from the device being used. If all the factors are Things You Know you might have a weak system with 10 factors.
3. The bank example also offers two factor authentication, in accordance with the VA. The first factor is the username and password. The factor that is on a separate system is the picture that is stored on the server side to ensure that you are logging into where you think you are logging into. (i.e. separate from the computer GAINING access)
4. What does the Tiger Team expect the Secretary to do with the recommendations for Stage 1 Meaningful Use? Will these recommendations be made into rules, or alternatively how will the Tiger Team recommendations be pushed out for Stage 1 Meaningful Use?