

Privacy & Security Tiger Team
Draft Transcript
July 24, 2012

Presentation

MacKenzie Robertson – Office of the National Coordinator

Thank you. Good morning, 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's also being transcribed, so please make sure to 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?

Peter DeVault – Epic Systems – Project Manager

Here.

MacKenzie Robertson – Office of the National Coordinator

Peter, thanks.

Peter DeVault – Epic Systems – Project Manager

Yes.

MacKenzie Robertson – Office of the National Coordinator

Leslie Francis? Gayle Harrell? John Houston?

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

Here.

MacKenzie Robertson – Office of the National Coordinator

Thanks, John. 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. Micky Tripathi? Latanya Sweeney? And is there any staff on the line?

Kristen Ratcliff – Office of the National Coordinator

Kristen Ratcliff from ONC.

MacKenzie Robertson – Office of the National Coordinator

Thanks, Christine.

David Holtzman – OCR – 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, Katherine. Okay, Deven, I'll turn it back over to you.

Deven McGraw – Center for Democracy & Technology – Director

All right. Terrific. Thank you, MacKenzie. We are going to spend the bulk of our call today, um, talking about Trusted Identities for Providers in Cyberspace. Um, just to sort of give a sense of, , where we are in our, in our timeline for working on these issues we—this is our last call, um, before the Health IT Policy Committee, um, which meets on Wednesday, August 1—so, um, just a little over a week from today.

Again, we're trying to reach some policy recommendations, um, based on what we learned from our hearing and in order to achieve trust for exchange of health information by providers in order to meet meaningful use. So we really are talking about a universe of transactions that are, that are, that are the ones that, um, are needed to it—um, for providers to achieve meaningful use. Obviously, there's a large universe of exchange out there but we always try to, um, be a bit more focused in our recommendations, which I think helps us actually come to some, um, conclusions.

Um, so again, this is our last call. We'll, um, you know, whatever we're able to get through—we have two hours today, but these are often complicated issues, so what-whatever we're able to achieve in the period of time that we have with, you know, obviously if there are some wordsmithing issues that we can, deal with, um, over e-mail we will, but I think substantively we have to do our best to try to get to what we think we can get to from a consensus standpoint in the time that we have today.

Um, one of the things that we've said from the very beginning is that we're trying to focus on solving trusted identity—deals with the issues of identity proofing on authentication and not necessarily the larger universe of, of sort of trusted access or actual authorization to be able to access data. So really the question is a-are you who you claim to be, um, and that, that by itself doesn't necessarily get you the keys to the data kingdom. Um, it's necessary; it's not sufficient, and, and it's very hard to keep ourselves focused on those sets of issues but I think we had, in our last call, um, done, done a good job of, of trying to keep these recommendations very focused, um, but also acknowledging that this is not—that solving this set of issues isn't necessarily, doesn't necessarily resolve all of, all of the potential issues.

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

Hey, Deven.

Deven McGraw – Center for Democracy & Technology – Director

Yes, John.

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

Um, could you go back to that last slide for just one second?

Deven McGraw – Center for Democracy & Technology – Director

Yeah, sure. Sorry.

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

I mean I, I, I, I agree with the question on the table, but I think that, um, what I heard in the testimony that I—and I'm wondering whether they should change the question a little bit— is, is are you who you claim to be with sufficient, a sufficient degree of certainty—

W

Assurance.

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

—assurance for, for the intended purpose because if you're gonna—the reason why I say it that way is because if you're gonna—you know, like the DEA may say for, for, for prescribing controlled substances you made the claim of who you, you know you are who you claim to be needs to be at a higher assurance level maybe than if you're accessing something for a lesser purpose. So does it make sense that—or does that just make it more complex than it needs to be?

Deven McGraw – Center for Democracy & Technology – Director

I don't-I don't think it does. I mean I, you know, I'm certainly comfortable with that. Does anybody have any disagreements to making that more clear?

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

I agree with him completely, and a lot of the discussion was around assurance, yeah.

Gayle

This is Gayle ... I agree with that as well.

Deven McGraw – Center for Democracy & Technology – Director

Okay. Thank you, Gayle.

Wes Rishel – Gartner, Inc.

So I have a question. This is Wes.

Deven McGraw – Center for Democracy & Technology – Director

Yes, Wes?

Wes Rishel – Gartner, Inc.

Um, the “You” in “are you who you claim to be,” is that a person or an organization?

Deven McGraw – Center for Democracy & Technology – Director

Well, and I, I think we'll get to that, um, because we—and, you know, as you'll see in some of the assumptions and recommendations we, we have sort of—the, the status quo is that the ‘You’ is the organization and—at least for exchange among disparate parties. And, you know, of course for exchange within an institution or an integrated delivery system, the “you” is, you know, do you have your, your individual credentials. And so the question really probably is—varies depending on maybe what's the model of exchange and, and the, the credential that you're trying to present. Is it an organization-level credential or is it a, an individual user credential?

Wes Rishel – Gartner, Inc.

Okay. Um, so, if I understand what you're saying, we are assuming— I guess I don't want to go that far. Are, are you saying that we're assuming that if we, if we have information or give access to information to an organization that we are assuming a certain level of assurance that the organization maintains about its users that, that may get access to that data or maybe the originator of the data as the case may be?

Deven McGraw – Center for Democracy & Technology – Director

Right. I think, I think we tried to address that in some—or I tried to in our draft recommendations, in the actual recommendations. The, the real purpose of just this slide is just to orient the discussion around, you know, that we're talking about trusted identity and identity assurance.

Wes Rishel – Gartner, Inc.

Okay. So my, my reason for, for asking this is that in several cases during the testimony I was, it appeared that certain, um, approaches, , were easier for individuals than for organizations—

Deven McGraw – Center for Democracy & Technology – Director

Right.

Wes Rishel – Gartner, Inc.

—or vice versa, and as long as we have that embedded in the discussion downstream I'm happy to wait.

Deven McGraw – Center for Democracy & Technology – Director

Well, let's, um, let's get to that downstream discussion—

Wes Rishel – Gartner, Inc.

Sure.

Deven McGraw – Center for Democracy & Technology – Director

--and if it's not sufficiently clear or if there are pieces of it that, you know, we need to flesh out some more, let-let's do that. That, that certainly was, you know, sort of in, in my mind as well, Wes, when I was pulling together, um, the draft in preparation for this call today and was certainly a theme of our last discussion as well, so.

Wes Rishel – Gartner, Inc.

Thanks.

Deven McGraw – Center for Democracy & Technology – Director

Okay. So, so what we, we have are some, um—we get to recommendations but, but, but this is sort of a—actually a slide deck that it is almost the way that if we're able to come to agreement today I would take, take the, the Policy Committee through, through the discussion, which is to acknowledge that, that what we have today is that organizations are responsible for credentialing individual users, um, within their EHR systems. Um, and although the HIPPA Security Rule doesn't require credentialing to be done at any particular level, one of the things that we did discuss on our last call is that we don't have, um, evidence to suggest that, in general, organizations are not taking this responsibility seriously or that there are widespread problems with this sort of delegated approach to trust and identity, at least, at least in the short term.

Um, but we also (again, this was where we were on our call last time) in the future we thought that ONC should, in fact, support individual- level provider credentials that at least met—meet the NIST level of assurance 3, which is LOA—you know, for members of the public who may not be certain is for level of assurance. And then, apologies in advance for the small type on the slide.

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

Um, before you start the small type—this is Dixie, Deven—, I think both the last slide and this one—, and I didn't think about it in the first early ones but, um, they, especially the one that you're showing right now, um—well, both of them. They, they seem to be all of a sudden diving within the organization, and I think that we should be very, very clear that we're talking about identity assurance between organizations. You know, in that last slide where you talked about, where it says, "Today organizations are responsible, um, for individual, credentialing individual users," it seems to lose the context a bit, and maybe we need to emphasize that that is our focus is between organizations.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I-I'm not sure it is just between organizations. Isn't really the ... separate questions?

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

Oh it—yes it did. Yeah, they made it very—if we're focusing on the hearing, they made it very, very clear that we're talking about between organizations.

Deven McGraw – Center for Democracy & Technology – Director

Well, but I think we get to make that choice, Dixie, and as you'll see—I don't know if anybody had a chance to read the document that I, that I circulated on Friday. Um, what, what I tried to do was to sort of lay out some different, um, scenarios, some different use cases, most of which do presume an org—you know, sort of exchange between or among disparate organizations. But there is one use case that reflects a previous Health IT Policy Committee recommendation that we teed up for them where we talked about remote access across a network that might not be secure, and that's not necessarily in-in-inter-organizational exchange.

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

Right, but it's not within the organization is, is my point. You're right, right, right. It's remote access and access between organizations, but it's not—we aren't looking, unless, I mean obviously our Tiger Team could be broader—looking at it broader than the hearing, but the hearing made it very clear that it was either—it was a remote access or between organizations.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Right, but it—, this is David. It all starts with individual identity assurance at some level, and that's what the focus is. And in some cases, that individual identity assurance would be asked by an organization.

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

I think you're opening up Pandora's Box by starting it at the individual level. I think that slide—

Deven McGraw – Center for Democracy & Technology – Director

Let's, you know, in many respects you guys are jumping the gun a little bit on me on these slides. These are, you know, kind of a step-wise set of arguments to get us to the meat of the discussion, which is clearly, um, where we all need to go. This is kind of laying out the fact that we at least acknowledged on our last call that an individual level credential that meets a, a certain high assur—a baseline high assurance level of 3 is really where ONC should be headed in part because that's where, um, other efforts are headed including DEA, um, and NSTIC. And it might be, um, a way to make it easier for providers to be credentialed with multiple organizations with whom they work on a regular basis, so.

Wes Rishel – Gartner, Inc.

C-can, —

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

Wes Rishel – Gartner, Inc.

Deven, can we just look at your in-the-future statement here and, and really only ask specifically what, what do you mean by it without—or would that be jumping the gun? I mean, is this gonna be restated in a more precise way further down in the deck?

Deven McGraw – Center for Democracy & Technology – Director

Well, I certainly tried to, Wes. I hope so. Um, that's why I sort of—I-I almost want to get us into the—to—

Wes Rishel – Gartner, Inc.

Yeah. Okay. That's fine. I'll just register that should is— should support is different than saying should require.

Deven McGraw – Center for Democracy & Technology – Director

Okay. Yep.

Wes Rishel – Gartner, Inc.

And that, um, absent our other discussions, it's unclear about whether that applies to someone logging in to use their EHR not—'cause ONC develops the certification requirements for EHRs.

Deven McGraw – Center for Democracy & Technology – Director

Right. That's correct.

Wes Rishel – Gartner, Inc.

Okay.

Deven McGraw – Center for Democracy & Technology – Director

That's correct. We can—we'll make sure that these intro slides match wherever we land from a policy standpoint, even if we go completely different than the straw recommendations that I, that I developed for you all. That's—these are just to—was an effort to help, help the discussion. So here I just want to quickly set the framework for where I thought we were landing based on our last call, but of course that's why we have these second calls is to, to, to, to re—you know, to have the discussion and see, um, , what recommendations, if any, um, we can achieve consensus on.

So the HIPPA Security Rule, as we know, again, doesn't set a specific requirement, so really at least single-factor authentication with, with existing ad-hoc organization-driven identity proofing is currently federal policy and, and will be at least for the short-term. But we had talked on our last call about moving to baseline, um, Level of Assurance 3 individual credentials, and I said ideally by Meaningful Use Stage 2 because that, you know, was, was something that was thrown out in the discussion, although admittedly we did not drill down on timeframes, um, very much on our last call because we didn't have a lot of time.

And, and here are some sort of suggested tiers, and then, you'll see—to getting to sort of full, , LOA NIST Level of Assurance 3 at the individual credential level, and then, you'll see on the next slide I tried to match them up with, um, some broad potential exchange use cases in healthcare. So Tier A is really the, the current state. You know, the baseline is, is, um, what, what organizations deem they need to meet the security rule, but it's generally from our understanding a single factor with the or-organization driving, um, the proofing.

Then Tier B is this sort of intermediate level where you move to the two-factor authentication but you still allow the organizations to drive, um, proofing. It should say, "Organization-driven proofing on the slide." There's a typo. And then, you know, you get to Tier C, which is, which is really the full baseline LOA 3 both on the identity side and the authentication side.

Again, we can discuss this. It's sort of three stages and then, an acknowledgement that the timeframe to getting to that full stage could vary. And in fact, arguably the recommendation can vary based on the privacy risk posed by the different exchange model or healthcare use case. So for example, the internal local access logon to your EHR, um, you know, clearly that's the Tier A, which is the current state, the baseline that we have today. And then, you know, whether or not that has to move to Level of Assurance 3 where you're talking about, um, internal secure access is, um, you know, like it is an open question, and I think even in these drafts I didn't, I didn't necessarily move us there.

But then, when you're talking about it, it, it's internal meaning it's, it's, it's within an organization or an integrated delivery system but the access is, is remote—um, which I think previously we had defined it as, as, as, a-across an unsecured channel like the Internet; we can drill down on that farther if we need to; that's obviously higher risk where we had said there should be more than single-factor authentication.

Um, you know, Tier B, again, is that intermediate tier where you move to the, to two-factor authentication but you still let organizations do their own identity proofing, and then, full LOA by the third tier.

And then, and then, we've got two use cases, um, identified here that are intra—inter-organization, um, either directed exchange where you're talking about exchange that is, that is to an intended end point from a data holder, and then an external exchange that involves a query or response across a network, and then the final use case is e-prescribing of controlled substances.

Now, these are, um, fairly broad use cases. They are not terribly granular, um, but I thought it might be a place to start. Um, again, on the assumption that, um, you know, based on our last meeting we're looking to, to move to individual-level credentials, um, by a certain timeframe, maybe that's the last stage of meaningful use. Do we need to do that for all use cases, I think, is one question on the table, and then, another question on the table is, is there a sort of staged way of getting from one point to another and, and in how much de—you know, how much detail can we identify that to, um, to the Policy Committee for it to, for it to consider?

So, you know, there are a few additional recommendations here, um, that we can and should talk about even in the short term where we're sort of relying on organizations to credentials or—and identity proof their own users. You know, it still would be helpful for ONC to continue its discussions, um, about achieving FICAM and/or Federal Bridge-level credentials for healthcare organizations. The open question that we keep circling the, the drain on—um, again, because we need the credentials that that are issued to be interoperable and, and ideally, um, accepted by the federal government.

And then there's, there's a few other things that I have teed up for your consideration, but I think we've got a lot on the table, um, and so I'm gonna pause there and, and let us start the discussion. I hope, I hope this make—that at least, that the framework that, um, that I did based on our last call at least makes sense even if you disagree with the margins. But if this approach doesn't make sense to you at all, we should talk about that too.

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

Deven, this is Dixie. I-I think it makes a lot of sense with one exception. I think, um, if you think about risk—and that's what security information ... because all that—your use cases on your Slide 7 I would not toss in, especially OCHA. I would not toss in OCHA with local access, and I probably would not toss in integrated delivery system either, um, because, you know, they're, they're usually vastly—you know the—they have facilities that are, um, you know, both integrated ID and ... consent facility, distributed facilities, all over the place. But, but OCHAs in particular often are comprised various, you know, legal entities that have come together, like, for example for an ACA, so I wouldn't—I would make that another use case, the integrated delivery system or OCHA or ACA—ACO.

Deven McGraw – Center for Democracy & Technology – Director

ACO, that's a good point, Dixie. Other, other comments either on the use cases, the tiered approach to getting to level 3, the idea of getting to level 3 at all, time-timeframes?

Wes Rishel – Gartner, Inc.

L-looking at the Slide 7 that's currently up, um—this is Wes—um, I, um, I hate to say this. Maybe Dixie or David could help me out but, but I'm not sure I understand what it means to use end-factor authentication for inter-organizational connections. , I mean, as far as I know there is a process for authenticating the other organization; it depends on a credential. And we want to know the level of assurance with which that credential was issued, but I'm not sure it even makes sense to talk about 2- or 3- factor authentication in that case does it? Am I just missing it?

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

Yeah. Yeah. It usually when you have a credential, um, your—that's your second factor. Y-you still have like a, a password, um—

Wes Rishel – Gartner, Inc.

Well, let's, when, when someone logs in—when a person, a user logs in—I understand that scenario. When the computer in the basement of the hospital sends information to a computer in a basement of another hospital, you know, using a daemon where there's no active user, it's not clear to me that, um, the, the, —there is the equivalent of a second factor. I'm just looking at the mechanics of what happens. If there is then I'd like to, I just—help me understand what it is.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think—this is David—I think that's why we need to separate those transactions that involve individuals from those that are system to system and not confuse the two.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

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

There are act—but there are actually three things, you know, like if it's—take TLS for example. TLS, um, server to client and—well no, both sides are authenticated. If it's—if it's mutually authenticated with TLS at both ends, they identify and authenticate themselves. But if you think about an IP-based, you know, um, IPV6, you know, VPN, I'm not—I think they identify themselves by IP address, but I think they only authenticate themselves by the credential or sometimes password. I don't think it has a point on, on that one.

Wes Rishel – Gartner, Inc.

Yeah. Okay. So we need to create, we need to—I-I think I'm reiter—I think I'm reiterating what David said, which is we need a set of discussions and slides that relate to users accessing, —and I'll say broadly health IT—we, we may want to limit to EHR—but users accessing at a minimum an HIE and a, and a portal of an HIE and an EHR, um, w-with—and levels of authentication. , and, and we need a discussion on intersystem machine-to-machine transfers authentication, which I don't think has changed based on what we've learned, and we need a discussion about proofing and a level of assurance for proofing. And there we, we need a, um, a discussion on the fact that the infrastructure for proofing is not well set up for proofing of organizations at this point—at organizational identities rather than individual identities.

I just had a thought maybe if I'm quiet it will go away, but would, would it be possible to, to proof the identity of an organization by proofing the identity of the chief privacy officer or the chief security officer or something like that? And as soon as I said it out loud I said it's probably not going to work, so never mind.

Deven McGraw – Center for Democracy & Technology – Director

So, yeah, but I thought that's how it did work.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. I think—I think that's practically what happens today is some official representing the organization is proofed.

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

But I think that we—this, this, this space is so complicated we have to be really narrow and kind of knock off very specific subsets that make sense and are unambiguous, as much as we can be unambiguous, and then zoom out a little bit and see what's left over rather than trying to accomplish everything in a sweeping statement.

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

I agree.

Wes Rishel – Gartner, Inc.

Yeah, me too.

Deven McGraw – Center for Democracy & Technology – Director

Yeah. Well, that's a great idea. Yeah. Um—

Wes Rishel – Gartner, Inc.

You've got a bunch of bottom-uppers here.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah, and it seems to me that the primary question that, that we've taken on, whether we were asked to do it exactly or whether we morphed it I can't reconstruct the history of how we got here, but the, the primary question is, you know, when an individual human authenticates to the system for, for a variety of purposes what level of assurance do we want for that individual authenticating to the system, and, , how do we get there given that we're—we agree we're not as, as strong as we should be?

And then a set of independent questions (important but maybe for another day) are if you have individually authenticated into a system and that system on your behalf communicates with another system, how does it carry forward your strength of authentication, and should it actually carry your personal credentials, or could it be an organizational statement that you're trusted because you met that organization's level of assurance? That, that latter question is important and hard and one we've put a lot of time and energy on because we were forced to in the discussions around direct exchange.

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

But doesn't—if the organization is trusted or there is some trust fabric that's established, that becomes—then that becomes a second factor in essence, correct?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, it is but you could say—you could define the, the definition of organizational trust is, for example, you must assure us that all of your providers authenticate with two-factor authentication. I mean that could be the definition of trust in a given network, and, and I'm saying that's a secondary question to us right now. The first question is what do we think the standard should be for individuals authenticating into systems containing healthcare data?

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

Yeah.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And I think we all agree that the state-of-the-art isn't good enough. We all agree also that it depends on the use case. Authenticating inside the hospital is probably different than authenticating from home, and it's probably different if you're authenticating into your own system versus a remote system managed by some other organization. And we've got those cases teased out here, and I like what Deven's put together.

Peter DeVault – Epic Systems – Project Manager

Folks, this is Peter DeVault. Um, I've got a question about scope, even if we carve out the system-to-system piece for a second and we're just talking about individuals, um, being credentialed to access certain kinds of functionality, to the extent that we are just talking about providers I think, , what we're discussing is a little bit problematic. There are a lot of work flows where support staff, for example, might be the ones who are actually doing the query and response or even the directed messaging, and if what we're really concerned about is those people being credentialed to perform those functions, then we've already moved beyond the providers.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah and it—I, I—this is David, Peter. I agree with that. I—and when I say provider, I really should say, you know, user of clin—user who has access to clinical data, 'cause I don't think it's limited to providers.

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

But I, I thin—I agree with both of you, a-and I think that, , Deven, we should, , try to capture that in our slides because that was a subject of a lot of discussion at the hearing.

Deven McGraw – Center for Democracy & Technology – Director

Yeah. No, definitely. I mean right, right now the way that it is captured is in a later slide. Um, we—it—what I put forward in draft was that there would need, need to be a discussion about how to, um, deal with proxy users (people who are accessing on a, on another person's behalf) as part of the NIST Level 3 framework, and that, that perhaps that's something that ONC could work with NIST on.

Wes Rishel – Gartner, Inc.

I think actually I wouldn't even—I, I think proxy is the wrong way to think about that kind of workflow.

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

I think so too.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

Wes Rishel – Gartner, Inc.

Um, there, there's—

Deven McGraw – Center for Democracy & Technology – Director

They need to acknowledge that there are, that there are users that may not be providers.

Wes Rishel – Gartner, Inc.

Exactly.

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

And it's care team we're talking about.

Deven McGraw – Center for Democracy & Technology – Director

Right.

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

But it still would have to be individually authenticated, but they may not be a, a provider; they may be another member of the care team.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Peter DeVault – Epic Systems – Project Manager

Or it might be a registrar. It could be somebody in the health information-management department. We're talking about—

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

Well, yeah.

Peter DeVault – Epic Systems – Project Manager

—... increase in the scope beyond providers.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. I mean it's—this is David again. I think it's a function of what they have access to, and this comes back to that original question of level of assurance with respect to what purpose that John raised at the very beginning. The focusing on providers is, in a sense, going after the highest risk use case, but clearly all of the others need, you know, a place in, in the spreadsheet somewhere.

Deven McGraw – Center for Democracy & Technology – Director

Well, right, although, although let's think about that for a minute. Is there any reason why we would—if, if the question we're focusing on is, is, is identity and authentication, why would we differentiate between one user and another?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, I mean, ask your, you know, ask the DEA why they have teased out physicians who write prescription for controlled substances. I think because they feel that's the highest risk group.

Deven McGraw – Center for Democracy & Technology – Director

Well right, but I also think that that's one where nobody else is allowed to write that script except, except the, the prescriber.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

But it's—that's why identity—that's why authentication is so serious to them is you have to prove that you are one of those people who has the privilege of writing those scripts.

Deven McGraw – Center for Democracy & Technology – Director

Well, that's right, but the, but that's a circumstance where there is a very narrow auth—you know, legal authorization for you to be in that space to begin with, right? As opposed to in other healthcare transactions where, um, you know, there might not be that sort of level of—

Peter DeVault – Epic Systems – Project Manager

I'd like to suggest that organizations will deal with a variety of levels of authentication that is, required, depending on a situation. For example, system operators that can change the level of authority of the user have to, have to use, two-factor authentication according to DEA. Um, and I don't think we need to specify once and for all for all users what is the required level of authentication as much as we need to find the exact range of cases where we do need to specify it.

For example, if we, if we want to make the statement and want the policy committee to make the statement that, that there should be a motion towards two-factor authentication for all users that either have access to healthcare data or are control of the authority of the system or something like that, w-we would say that would be—we'd be moving towards that as a minimum level. Or, or we could say move towards supporting it but not moving towards name level.

But as far as getting into whether this physician needs a different level of authentication when they're signing an order for a controlled substance and when they're signing an order for aspirin, um, I, I don't think w-we need to—I don't think we want to get in to that level of, of diddling.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Leslie Francis – National Committee on Vital and Health Statistics

This is Leslie. I'm sorry I joined a little bit late—um, Leslie Francis. But this is an area where it seems to me that the question of who can see what versus authentication is what's really driving some of the issues here because once you expand the range of people who get credentials beyond physicians and other licensed providers you, you've in some sense wildly opened the door. But organizations are, of course, going to need to have admitting clerks and other people like that be able to have access.

Peter DeVault – Epic Systems – Project Manager

I think we're, we're—this—at least for this meeting we're just focusing on how.

Leslie Francis – National Committee on Vital and Health Statistics

Right.

Peter DeVault – Epic Systems – Project Manager

We're, we're not focusing really on, on being sure we know the iden—what level of assurance we have to know the identity. We're not focusing on what—

Leslie Francis – National Committee on Vital and Health Statistics

I know.

Peter DeVault – Epic Systems – Project Manager

—what level of assurance is required for which use case.

Leslie Francis – National Committee on Vital and Health Statistics

Oh, no. I know that.

Peter DeVault – Epic Systems – Project Manager

Oh, I guess we are. Never mind. I better shut up here.

Deven McGraw – Center for Democracy & Technology – Director

And I know it's—I mean I think I see, um, I think I see Leslie's point, which is that if we're suggesting that let's say in the query/response use case, for example—query response across a network—um, where you've got sort of, um, , professional staff below the level of provider with, with, with a, with a Level 2 credential, does that necessarily mean they get to access data from another institution even, even if they, you know, present an appropriate credential that says they are who they say they are.

You know, again, that's—I think that gets back to the threshold ques—um, statement that we made at the very beginning, which is to say, you know, resolving questions of identity, , and, and, and assurance, some level of assurance of that identity does not necessarily translate into, um, automatic access.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. And this is David. I-I think that's—it has to be—I mean, that is completely self-evident. It's principle number one. If we feel the need to state it, we should state it just to prevent people from being confused. But the worst possible case is when you have users and you don't know who they are, right?

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

If you know who they are, then you can make rational decisions about what they're allowed to do. If you don't know who they are, all bets are off. So you, you can't take that and turn it around and say, "Just because I know who you are, I therefore let you do anything."

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

That's, that's a complete non-sequitur. It has to be, "I have to know who you are before you can do anything." And then, we will say, "And I have to know it with certain degrees of certainty depending upon what you're asking to do—certain degrees of assurance depending on what you're asking to do."

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

So I mean it, it is, it is—it would be really counterproductive to say we shouldn't assure identity because that would increase the chance of people doing things they shouldn't do. That—I mean that's completely non-sequitur logic.

Leslie Francis – National Committee on Vital and Health Statistics

Oh, yeah. I wasn't meaning to suggest that. I—this is Leslie again—I, I just thought the way the conversation was going the two questions were getting linked up again.

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. No, I think you made a great point. I'm just, I'm just being definitive in saying we, you know, we—

Deven McGraw – Center for Democracy & Technology – Director

We can't go there.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

We can't go there. We have—w-we, we're debating how certain should we identify h-how—w-what level of assurance is appropriate and what's our definition for those levels of assurance. And if we think everybody should be the same all the time immediately, that's going to be a big cost on the healthcare system. If we think we should stage it carefully over time, then we have to do a little bit of parceling out by use case and role, , simply because that's what we have to do if you just—if, if you say, not everybody has to get there all at once.

I mean it would be nice if everybody had full-blown Level 3 three assurance tomorrow morning and nothing was allowed to happen in healthcare until that was achieved, but we know we can't go there so we have to, we have to back off and break it down into these stages. And I-I think what Deven was trying to do was to decouple the NIST Level of Assurance 2 from Level of Assurance 3 and create kind of a way station in between those two that makes sense in healthcare given that healthcare organizations already do a pretty good job of identity proofing even though they don't do it according to NIST's defined rules. They do it according to JCAHO and best practice and their own internal risk assessment about, you know, having rogue users on the system. Healthcare organizations proof their users pretty well.

So we're—we're proposing here that there's a Level of Assurance 2 and there's just kind of a fuzzy 2.5 that we're carving out where it's two factor for authentication but non-, non-NIST proofing, and then, there's Level 3 for proofing and multifactor that we would get to by Stage 3 and that—

Peter DeVault – Epic Systems – Project Manager

I'm sorry, what, what is, what is NIST—what is in NIST Level 3 that healthcare organizations don't do?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, the li—NIST Level 3 has some very specific things about number of government IDs and verification of those IDs, and I suspect that healthcare organizations don't follow the letter of the law on that.

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

No, it—

David McCallie – Cerner Corporation – Vice President of Medical Informatics

They validate—they—

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

No it's—I think you should look at the latest one. It has—at least one needs to be a government issued picture ID, but quite frankly I think most healthcare organizations do that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, I think they do but I don't think we have a—

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

Yeah.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

—we don't have a process to—

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

They don't say, like, you must have two or three. They say—

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Right. And it's, you know, NIST makes a clear point. Their document is for government use. It's not for healthcare.

Peter DeVault – Epic Systems – Project Manager

It would—they describe their levels operationally, right? I mean, I, I, I think it's worth examining whether we think that healthcare organizations ought to do NIST Level 3. Um, you know, and if some are doing it now and some aren't, then there obviously has to be a transition period. But I-I would—

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, we heard in the testimony that, that organizations certainly aren't—they don't consider that they're doing it. The, I forget his name, the Washington—

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

Rick, Rick Rueben.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Rick Rueben. I mean he—you know, they, they do not have specific standards for their organizations. They ask the organizations to, as he put it, “Do the right thing.”

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Now it may well be that, that, that their internal do the right thing.

Peter DeVault – Epic Systems – Project Manager

Yeah. So I suppose the practice—you know, the question is if a practice hires a medical assistant which is not a licensed physician, should, should, should they be checking the government photo ID is that person or not.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And the financial statement and validating it with the, the—

Peter DeVault – Epic Systems – Project Manager

Oh, that’s part of NIST Level 3?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

That’s part of NIST Level 3. And I, I’m not sure they do that for every person in those settings.

Peter DeVault – Epic Systems – Project Manager

Yeah. Okay. Well, then, then that answers my question. Well, and act—I didn’t know—I-I forgot about the financial statement. I—yeah.

Deven McGraw – Center for Democracy & Technology – Director

Yeah. So I think—I think there are sort of two sets of issues on the table that we appear to be talking about simultaneously. This is Deven. One is, um, whether there ought to be a sort of middle tier in getting from current state to, um, NIST LOA 3, um, which we certainly defined in middle—in the, in the, in the draft. But that’s one set of issues to discuss.

The other one is to identify from the, the chart on Slide 7 what are the particular, more risky, use cases where we think it’s just—it—we think there ought to be, um, Level 3 for individual, um, authentication in, , you know, for authentication of an individual user.

Um, we were starting to sort of play in that sandbox and then left it to talk about sort of how we would tier to get to Level 3, and I think, I think if we can get a more clear answer on those two questions, we’ll be in pretty good shape.

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

You know, Deven, this is Dixie. Um, the NIST 800-63, , starts out by defining the risk that each of the levels is intended to counter, um, and I think it would be worthwhile for everybody to know what those definitions are, um, a-as kind of a framework for figuring out where the use cases fit. I-It sounds almost like we’re trying to come up with our own definition for what the risks are, you know, for each level, and it seems only reasonable to start with what—how they’ve defined them.

Deven McGraw – Center for Democracy & Technology – Director

Well, it—I-I’m not suggesting that’s a bad idea, but our model is based on what we know about healthcare, whereas NIST is not specific to healthcare.

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

Right. I know, but I meant to plug it in for ...—

Deven McGraw – Center for Democracy & Technology – Director

And this ... just the very beginning that what we wanted—, even when we had the discussion around these issues months and months ago, well before our hearing, what we wanted was a high level of, of assurance, which would have, in fact, landed us on Level 3, but we weren't fully comfortable with the, with the elements that would be required in order to achieve that level based on the prior iteration of 800-63.

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

Right.

Deven McGraw – Center for Democracy & Technology – Director

I—to me I read those NIST risk levels and they don't answer any of those questions.

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

Okay.

Deven McGraw – Center for Democracy & Technology – Director

What, what's the typical healthcare exchange use case, at least in a general term, that, that, that, that raises more risk than the, the internal access within, within a, within, um—you know, which is onsite logging into the EHR within my institution, um, versus logging in remotely versus being able to q-query and access information across a network, um, all the way up to e-prescribing of a controlled substance.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And I, I think—don't we all agree that there are different risks associated with those use cases?

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

Sure. Sure. Absolutely.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

So it doesn't, I mean, at least on—

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

... we, we look at what the risks are and see how they plug-in to something that already fits, but if we want to just create our own that's, that's fine too.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And, and I think we are trying to plug into the NIST framework. I mean, you could ask the question of whether we need to define our own parallel equivalent to NIST because NIST doesn't use healthcare-specific examples, um, but I—given that we don't have that, um, you know, using the NIST model and just making the analogy seems—it seems like a parsimonious course. Maybe one of our recommendations should be to consider creating a, a healthcare-specific equivalent to the NIST, Levels of Assurance 2 and 3 and 4 but—

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

I think, I think you're idea of creating four examples that are specific to healthcare is a great idea.

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

You know, so you might say, you know a risk of, —a risk addressed by Level 3 might be the risk of unauthor—of spoofing of identity and the ability to query patient medical data from outside of a, of a system. I mean, that might be something that your Level 3 is intended to prevent.

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

Except it's not intended to prevent a man-in-the-middle attack. That, that's—I mean—

David McCallie – Cerner Corporation – Vice President of Medical Informatics

But I didn't say that. I said—

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

No. No. Let's look at the map when we get it dismantled.

Deven McGraw – Center for Democracy & Technology – Director

Yeah. And, and, and, and so, Dixie, you just actually landed on one of the things that's gonna be a struggle for other members of the Policy Committee without, um, cryptographic expertise. We might have a couple of people who know what a man-in-the-middle attack is, but not a lot. So, so we have to, we have to speak in the language of healthcare policy for this particular set of recommendations and have them make sense to a policy audience.

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

Um-hmm. Um-hmm.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And that's, that's why referencing back to the NIST standards is useful because that, that reflects—even though it isn't healthcare specific it reflects a tremendous amount of thought by people that do this for a living.

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

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

Um-hmm. Yeah. That's exact—that's all I was saying. They don't have healthcare examples but we can provide those.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. We—maybe that's, that's one of the, you know, things we could do.

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

Yeah.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

So, you know, kind of picking up on Deven's thread of, of if, if we agree that there are different levels of risk, is it—does it make sense to try to stratify to a couple of, kind of group or categories of levels of risk—even though we won't enumerate all of them because there are thousands of use cases in healthcare—but could we come up with some of these broad categories like Deven's tried to do in Slide 7 and, if so, what are they? And I-I think the ones in Slide 7 are, are—you know, it's a good start.

Judy Faulkner – Epic Systems – Founder

This is Judy and I agree with you very much on that one. I think that to put it into different categories and then to let the healthcare org—because we can't, um, figure out every use and how, , how critical it is or dangerous it is—to let the healthcare organizations figure out themselves how they divide it into those different groups.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. So, you know, the initial—this is David again—the initial group that Deven describes as internal local access on site, I think we kind of have a notion that that's access via devices that are in a physical location where the access could be observed and is or de—and they are devices that are inside an organization's firewall—in other words, the traditional healthcare organization with the terminals. Maybe that's a diminishing use case given that people are using wireless devices everywhere but let—it, it's still pretty common.

And that makes sense as your kind of, um, you know, most secure starting point. In a sense, the physical location of the device and the fact that you're inside the firewall gives you a reduced risk of someone misappropriating data. That, that—

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

I think that, I think that the physical confinement is really important.

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Right.

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

You know, because once you allow a wireless output a-access, it's not, you know, a local access. It's a very—

Deven McGraw – Center for Democracy & Technology – Director

No, that's fair, Dixie, and I'll definitely take that little start.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. Maybe say, “Physically connected” or something like that, non-wireless. I'm not sure.

Deven McGraw – Center for Democracy & Technology – Director

Maybe it might be more important to sort of throw out what we mean when we say “remote,” where we think, you know, that there are enhanced risks. And just to remind us of where we were before on this question, we, we landed on, um, you know, through an unsecure connection like the Internet, I think.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Sure.

Deven McGraw – Center for Democracy & Technology – Director

But Linda, Linda Koontz, does that sound like—am I right about that? Do you remember?

Linda Koontz – MITRE – Principal Information Systems Engineer, Privacy

Yes.

Deven McGraw – Center for Democracy & Technology – Director

Okay. Thank you.

Judy Faulkner – Epic Systems – Founder

This is Judy, and I wanted to comment that not only, , may wireless be iPads carried around but wireless could—is also the ubiquitous, um, workstations on wheels that are wheeled around, and so in, in a secure environment wireless would be all over the place. So we have to be very careful of that definition.

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And, and I wonder maybe that—this is David again—that the definition is not so much wireless or non-wireless but whether the access is from within inside the firewall or coming across the firewall. And I'm, I'm not sure if that's technically a feasible definition. Dixie, does that make sense to you?

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

No. Um, to quote the great Wes Rishel, we had, we had this conversation in the Privacy and Security Workgroup some time ago, and he came up with some words about, um, where the possibility of if it's going over an unprotected network, it cannot be eliminated. So, so you really have to think about, um, from getting from here to there is it, is it possible at all that it could possibly go over an unprotected network either, either, um, physically protected or encrypted protected? And if so, then it requires an additional level of protection.

Deven McGraw – Center for Democracy & Technology – Director

And, and that's even relevant in the context of, of identity, secure identity.

M

Yeah. It's a different issue.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, it's a risk. It's a, it's a staging of risk which we're then going to map to need for level of assurance.

W

Yeah.

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

Yes. That—, I meant—yeah. Yeah. This is kind of the second—the higher risk is where there is a possibility that, that that—you know, your password could be exposed, let's say, right.

Deven McGraw – Center for Democracy & Technology – Director

Right or you could—

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

... authenticator could be exposed. That's a higher level of risk.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

You know there's a—another category that I think we're seeing more commonly these days as, , wireless devices become bring—um, as you have these bring-your-own devices, which is, you know, an emerging trend, is the a-attachment of secure identity to the device itself. The devices become credentialed so you can prove that it—that the access is from a device which carries a credential. We're starting to do that and that, that's yet another factor that's not common yet, I don't believe, but I think it will see—we'll see more of that as, , as yet another tier, if you would—um, is the device verifiably a credentialed device or not

Leslie Francis – National Committee on Vital and Health Statistics

This is Leslie Francis. One of the—this is the most low-tech of points. If you can see the person physically doing it, then there's somebody there to check up on who the person is. So with that possibility, you can have a credentialed device somewhere else and somebody around the house picks it up and logs in.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. Right. No, I think that the coming across the firewall is, is you know, is, is a critical factor. It's coming over a public network. Credentialed or not you've got to proof the user, but inside the hospital a credentialed device that's not going across the firewall may be treated differently than a non-credentialed device not going over the firewall.

Leslie Francis – National Committee on Vital and Health Statistics

Right and a lot of those devices inside the system would be—potentially could be treated differently from a wireless device that's in my house.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Right. That's why I think that the point that it's wireless becomes somewhat irrelevant.

Leslie Francis – National Committee on Vital and Health Statistics

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I mean it, it's really more what, what like Dixie and Wes were saying, it's which—does, does it go over a network or not, and do you know anything about this device or not? And then, of course, those all set you up for a level—for a question of how, how, how much work does the user who claims to be—who's using that device have to assert who they are, what, what level of assurance depending upon those other factors? So it's, it, —, the point is that there could be a lot of subtlety in here, and I don't know how we'd draw the line at, at broad categories.

Deven McGraw – Center for Democracy & Technology – Director

Well, I think we do the—I think what, what we appear to be doing (and it seems like an appealing way to prevent this from a policy standpoint) is to come up with some use cases that we know are common for it, and, and will likely be common for exchange of data among healthcare providers in order to meet—to meet meaningful use. And so, you know, one of them is, you know, sort of, you know, use of a device, um, in order to access the network, right?

So we—and, and, and these, these sort of scenarios present some higher level of risk than the sort of traditional, um, you know, within the physical confines of the, of the facility or the office practice that, that's, you know, rapidly becoming, um, somewhat dinosaur-is but with, with a lot easier to, to control and maintain.

And we are looking for, you know—and, and it almost sounds like (but I could be over reading us) we're almost looking to identify a, a sort of set of scenarios where, you know, we ought to get to, um, individual users being credentialed at Level 3, um, you know, by Stage 3 of Meaningful Use. Am, am I reading this right?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

State the question again, Deven. I got distracted. I apologize.

Deven McGraw – Center for Democracy & Technology – Director

No, it's okay, and I probably was not as clear as, as I wanted to be. So we—so where, where it sounds like we're, we're starting to land again, sort of picking up on where we were heading in our last call, is that, you know, where you're talking about what's going to be needed to have assurance of human user authentication, um, and when we would want to see it be at Level 3, we're sort of identifying a class of, of, of, you know, some scenarios. One could say remote or, or non-physically confined types of access that might—that, that would justify needing a, a higher level of, of assurance on that authentication, you know, 'cause it—

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah.

Deven McGraw – Center for Democracy & Technology – Director

Does that sound right? I mean, it's just really hard to describe this stuff but I, but I'm trying to sort of—

David McCallie – Cerner Corporation – Vice President of Medical Informatics

So, Deven, to put it—

Deven McGraw – Center for Democracy & Technology – Director

—but in a realm of sort of policy-type use cases that doesn't have us drilling down with excruciating detail.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

So, so I think if I, if I was to put it in—what you said in—

Deven McGraw – Center for Democracy & Technology – Director

Into better words, please, David.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, into different words that are not—that are, that are more policy level is we believe that there are, in fact, different levels of risk that warrant different levels of assurance en route to eventually arriving at Level 3 of assurance for all clinical users.

So we've really got kind of two—two questions here is, is, is do we believe that we could stage this based on, on really one major question: Can we stage the progression to Level 3 assurance based on risk stratification? And I think we're saying we think we can and that we can get there without disruption to the healthcare industry by careful attention to the staging, taking into account risk stratification, so—such as the difference in risk between a local user under observation at a nursing station with a directly wired device, on the one hand, and remote use of a personal cellphone from home into a, a community HIE on the other extreme.

So we think there are differences in risk in those use cases that, that can be stratified into a number of areas and that the, the speed with which we reach Level 3 assurance could be cast in terms of the, the—, as a function of those levels, of those different stratified levels of risk. I mean, that's pretty abstract way of saying it but I—is, is that not what we're roughly saying?

Deven McGraw – Center for Democracy & Technology – Director

I—that's what it feels like we're roughly saying, although, I, I think the one piece that I still have a question about is whether we need or want to require a Level 3, um, indivi—assurance even for the sort of access within the physical facility—that sort of first tier—um, assuming that the definition of local really is what—you know, within an organization.

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

Yeah. I say—that's what I was thinking, Deven. You know there are like instances like, like DEA has already de—has already decided that, , if you're prescribing controlled substances, the level of risk is high enough that it needs two factor. Well, I think things like breaking the glass is something else. Even though you're in a physical facility, I think, you know, to break the glass and access something that you don't have access to as a physician should require two-factor authentication.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, do we—did, did you guys hear Farzad's opening statement to mean that Level 3 assurance would apply everywhere, even including routine access in the hospital? I mean I can—

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

Yeah. I sure didn't. I thought—and I just re-read it.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

This is Joy. The answer is no.

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

What—weren't they talking about, Joy, I can't find it written, um, that, that in the hearing it was really remote access and access between organizations?

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Yes. It is remote, and we do recognize—I've been liv—I've been on this call and have noted that the, the definition of remote is difficulty—is difficult—

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

Um-hmm. Yeah.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

—particularly as some of the issues that David and you raised, um, which are, you know, so how do you treat cell phones when they're in a hospital? How do you treat WiFi when it's in a hospital or when it's in a provider's office if, you know, if you have the potential for people sitting there being able to access it readily? It is a little bit different situation than somebody logging onto a, you know, a hard-wired computer system.

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

Yeah. I'm a little concerned, Deven, that—this is Dixie. I, I think this is the crux of my concern. Up to this point, we really haven't interfered with how organizations run their own show—

Deven McGraw – Center for Democracy & Technology – Director

Right.

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

—and, and I think that we should be careful not to do that here. Um, so I, I would be much more inclined to define these use cases not in terms of whether it's one organization or an OCHA or, you know, or whatever, , but, but rather in terms of whether, whether the authentication data are ever put at risk—you know, the level of risk. You know is it wireless authentication? Is it, um, is it, is it authentication within a— is it somebody else mentioned where you can see somebody, you know, um, within a facility? But not phrase it in terms of, you know, IDNs, single organization, OCHA or whatever.

Deven McGraw – Center for Democracy & Technology – Director

Yeah. No, that's, that's fair, Dixie, and that's going to come out of the slide. I, I mean, I don't have the capability to remove it right now or I would.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

So can I, can I come back to what Joy said a minute ago and, and in response to the question about what Farzad meant? So, Joy, let me turn that around as a affirmative statement.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Okay.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

You—ONC is comfortable that single-factor authentication inside the healthcare organization is sufficient for routine connected observed care, I mean; this is the lowest risk profile? I mean, do—are we saying that we don't think we need to get to Level 3 assurance for the use case of the—in the hospital?

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

I would say that we don't—we do not believe that needs to be addressed at the moment. How's that? Is that fair?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Okay. Yep.

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

That's what I was picking up at the hearing.

Deven McGraw – Center for Democracy & Technology – Director

Yeah. So, so if we were to sort of lift this conversation up a level, it almost sounds like what we're recommending is to reach, um, individual assurance, LOA 3, for, um, access, um for access between organizations or remote access to an individual across an, a-a-across a firewall or, , unsecured network.

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

Just across a network and then we'll, you know, get down to the detail.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Oh, across a remote network?

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

Yeah. Yeah. Yeah. Or—yeah, yeah, yeah. But it can be wireless as well.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Any network is potentially remote, right?

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

This is tested. A, a network that's—where there's any possibility of—if ...

David McCallie – Cerner Corporation – Vice President of Medical Informatics

... one internal network, because you—yeah, internal net—even internal wireless networks though will have adequate security so that you can, you can—I don't think you have to worry about Level 3 but once you go outside your shop and, and—that's why I think that's where it applies, I think.

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

Yeah. Yeah. External or wireless—external wire-to-wireless networks.

Deven McGraw – Center for Democracy & Technology – Director

And so in that case we're looking—we're, we're recommending that, Level 3 credentials be in place by Meaningful Use Stage 3, and we are suggesting that one phased way to get there would be to have sort of an intermediate level that isn't quite NIST compliant on the identity-proofing piece but is NIST compliant on the authen—on the two-factor authentication, which is now a bit easier to, um, achieve given that, that, um, modifications to NIST 800-63, um, and the use of, of m-mobile in particular to, to issue, um, a credential. Is that, is that—maybe we don't want to go into the mobile thing, but there, but there are expanded options for reaching Level 2 authentication, which did not exist a year ago when we were having this same discussion.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

You mean two-factor authentication.

Deven McGraw – Center for Democracy & Technology – Director

Yes. Thank you.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And I, I think that maybe a little footnote—I. I mean, I agree with what you just said. I think a little footnote is that, you know, NIST may need to be engaged in evaluating new technologies as they emerge to include them within the acceptable set of—

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

—two-factor, second factor, because undoubtedly there'll be new things coming.

Leslie Francis – National Committee on Vital and Health Statistics

That's very important given the criticism of passwords that we heard at the hearing. This is Leslie.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, there are also NIST rules about password, or at least suggestions about passwords, and risk associated with, you know, strength of passwords, number of, , attacks where you exclude—we, , and are we factoring that in as well and saying that should be a part of the package?

Deven McGraw – Center for Democracy & Technology – Director

Well, I mean, I think what we're, what we're doing is, um—I mean, we're asking for ONC to get to Level 3, which sort of gets you out of r-reliance on passwords but certainly, you know, continuing work on password strength since that's going to be, um, y-you know, at least utilized for some forms of authentication less—in less risky scenarios for—and, and also as we sort of move to, um, you know, Level 3 the, the, the, the use of user name and password is still gonna be the general operating—to be MO.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. I mean, password is, is one of the factors. Even in two-factor authentication the password is, is—can be one of the factors and, and NIST does a good job of defining what a good password looks like or at least, you know, giving you some way to assess the difference between good and bad. I don't think they put a line in the sand and say, "Above this is good," but they give you some guidelines that are, you know, pretty thoughtful.

Judy Faulkner – Epic Systems – Founder

This is Judy. I wonder if we can talk about the cost rule this year so that we take that into consideration as we do this. If they need something issued by NIST, I think there's a cost isn't there to be issued something by a NIST delegate? And then we have the cost of, um—every single place if you want their biometric recognition, it's the cost of whatever the appliance is to be the reader at ever place that it needs to be read. And just a quick calculation, an organization with say, 6,000 users, (which is a large but not gigantic healthcare organization), um, I calculate—and this may be wrong because I, —but it's gonna be maybe 400 hours a day of time if there's an extra password to put in.

So those are things that as we figure this out we should realize that the healthcare organizations are probably going to be calculating that themselves as they, as they look at this.

Deven McGraw – Center for Democracy & Technology – Director

Right. Well, I think we should definitely say something about cost. I—you know biometrics are not—I think are not even covered in NIST 800-63, so—

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Deven, this is Joy. That's correct. They don't recognize biometrics as a factor at this point.

Deven McGraw – Center for Democracy & Technology – Director

Yeah. So us moving to, to, you know, having a recommendation on the table that, that, that urges ONC to move to Level 3 for remote exch—you know, for remote access or, um, exchange across a remote external exchange, external wireless exchange, um, that that's not gonna trigger the biometric issue.

I think we should though mention that we did, at the hearing, get some testimony about cost that suggests that it's low but it's, you know, we don't— I don't—it, it clearly the, the solution has to be one that, that's low cost.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Yeah. Deven, this is Joy. I'd also like to clarify that NIST you don't have to—, NIST is a standards setting. It does not issue anything.

Deven McGraw – Center for Democracy & Technology – Director

Yeah. They don't issue credentials; that's right.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

They don't issue credentials and, , the, the, , update to 800-63 that was issued in—I think it was December of last year—recognizes a lot of different technologies within two-factor authentication including, you know, one-time password on a cellphone and, and things of that nature. So it's, it's much more liberal than it was the last time that we took up the issue.

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Although there are some surprising things that they don't accept or they don't recommend such as knowledge-based challenge questions from public sources, which was an interesting—I didn't realize they'd gone to that, which I think makes sense, but that's in common use by, say, banks and other sources and wouldn't qualify. Knowledge-based from private data is okay but not—

Deven McGraw – Center for Democracy & Technology – Director

Yeah. I mean, I agree with you David. I think it makes sense. It's interesting that that the — that challenge questions from public data are still allowed to be used.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And you—you did see the recommendation that you—when you name your first pet you should at least use a character some uppercase and a couple of numbers.

Deven McGraw – Center for Democracy & Technology – Director

No, I actually missed that. Well, there goes Spot.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. That—

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

Now Spot exclamation point is okay.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Right. Spot-one-exclaim-pound, that's okay.

Deven McGraw – Center for Democracy & Technology – Director

BadSpot exclamation point!

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

Yeah.

Deven McGraw – Center for Democracy & Technology – Director

So let me, let me—so in other words, um, I, I think we can frame a set of recommendations that calls for moving to LOA 3 individual-level credentials by Meaningful Use Stage 3 for the set of, of sort of riskier transactions that involve external exchange and remote access. We can, we can sort of lay out some scenarios like the ones that we raised on phone but also acknowledge that this may need some further, um, exploration in order to sort of define the, the, the more riskier set of transactions, with a larger risk in the identity space really being about proofing—that, that, that the person is—claims to be someone, but in fact it's, it's someone who has taken their credential and is, and is using it, which is, um—which when you're only relying on passwords, um, is, is more likely to occur. Is that, is that fair?

And, and then we have an idea for moving to LOA 3 NIST, NIST LOA 3, which is this sort of middle tier where the identity proofing, um, is, is permitted to be organization driven and not, um, NIST com-, , compliant but you, but you have the, the two-factor authentication.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

This is David. I, I like that. I, I also wonder if... this—back to your first point—this sort of categorization of these risk levels, is there an activity that Standards Committee or some other body should take on to try to kind of enumerate some of these healthcare risk strata?

Deven McGraw – Center for Democracy & Technology – Director

I think that's a terrific idea. Are, are, are you—, and I would love to delegate it to the Standards Committee.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Well, I—and you know the Standards Committee usually turns around and delegates it to the S&I Framework or something like that. But I, I'm just wondering if—do we—is it worth pursuing through whatever channel a more concrete enumeration of these, or is this just common sense and, and are good practices—we, we know how to deal with it? I think it, you know, I think the larger organizations understand this pretty well. I'm not sure all healthcare organizations do.

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

I, I wouldn't even say that large—I—my—but I, I think that the Privacy and Security Workgroup of the Standards Committee would be a good place to do that, yeah.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

You, you—that's your workgroup, so you just got it.

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

I mean, it has to go through the committee obviously to get assigned to us, but I, I do think that, um—yeah, I think people in that workgroup would be, , you know, would be good to do that, and, and express it in ways that, that the average human on the street could understand.

W

Yeah.

Judy Faulkner – Epic Systems – Founder

What about making sure that it includes at least a few people who are physicians who have actually done this sort of thing so they could put a reality check in their mind—

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

Well we—

Judy Faulkner – Epic Systems – Founder

—and who, who will show up at these meetings or on these calls and participate.

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

We wouldn't be recommending the solutions. I think what we're—what I'm, I'm volunteering to is just to kind of a continuum of risk, scale of risk from least to highest, and then it would come back to the Policy Committee.

Judy Faulkner – Epic Systems – Founder

Yeah. And that's what I'm saying though. If we really want to get a, a good real scaling of the risk, I think having physicians who are users of that sort of thing will be able to see that better than anyone who's trying to put themselves hypothetically into this situation.

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

Sure. I think that's a great idea.

W

Yeah.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. But I think Judy's—I think to Judy's point though I think it's not so much the physicians for risk purposes but frankly adoption, which is going to be pr—I continue to think it's going to be one of the biggest issues here is whatever we, we propose has to be something that's going to be adoptable and it's going to be supported by the physician community.

Deven McGraw – Center for Democracy & Technology – Director

Yep.

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

And, and we all—and we know that part, part of—a huge part of getting physicians to adopt anything, whether it's security or not, is to make sure that they understand its value to us, so—to them, and so I think that, , yeah, that, that defining what, what the real risks that the policy recommendations address is really important toward adoption. I, I agree.

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

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

At the end of the day, we can, we can talk about risk all day long but if physicians sees it as, as imposing a, a step for a couple seconds in a, on a process they do multiple times a day, you'll get a lot of passive, you know.

Deven McGraw – Center for Democracy & Technology – Director

Yeah and workarounds. Yep.

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

Yep.

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

Well, and that's, you know, yeah. A-and it's not all security risk, it's also safety risk. So I think that, you know, both of them have to be factored in.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And that's why—

Deven McGraw – Center for Democracy & Technology – Director

I mean, one of the things we can say is, you know, we can ask for the Standards Committee to do some work on the, the, the, sort of, use cases that it, that, um, involve, additional risk, and, and, and—but also note that, you know, w-we constantly need it to be, we need to be looking at the impact of these policies on, on workflow and whether users ... are creating workarounds in order to avoid the additional, you know—that there ideally should be ways to do this from a technology standpoint that don't involve enormous hoops that people have to jump through because if it's—if the impact is the latter then we're, we'll be done, I think.

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

Well, I think it's reasonable to say that, that this, that this, um, scale that we're envisioning should include—should address both security risk as well as quality and safety risk because in our environment both of those are really important and they're not always, um, you know, aligned. But it is important whenever you do any, any security, um, countermeasures in, in a health environment you have to consider the, the safety and quality risk.

Deven McGraw – Center for Democracy & Technology – Director

Yep.

Judy Faulkner – Epic Systems – Founder

And that's why I think it's good to have the doctors involved because you also need, , the physician adoption, and if they don't believe it's a security risk—if we do but they don't—then they're not going to adopt it. They have to believe in the same thing. That's why they're saying this is going to be important because they're the ones who may be 20, 30, 40, 50 times a day have to do this, and they have to buy into it.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Well—this is Joy—um, I think that's accurate, but I think there are two different ways of looking at this. One is are you going to set your standards, based on what people are willing to do now based on their current perception, or are you going to set the standards and then have education to convince them that this is the right way to go?

Judy Faulkner – Epic Systems – Founder

But I think if they live it every day they will know, and I think they are concerned enough that they'll do the right thing. That's been usually my observation with physicians, so.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Well, we are—yeah and, and I don't—I'm not sure where you, you're headed with this. Do you want to have another hearing on it? Do you want people to come in and talk to you about what they've done? I know Mark Frisse, the hospital organ—the enterprise that he was involved with actually did two-factor authentication, and there are several examples that have.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Well no, I'm—where I'm going with this is just what was proposed earlier that if there is a group who's going to review it and try to come up with the risks, and what should be done that that group include, , practicing physicians. That's all.

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

No. I think we're getting way ahead of ourselves, because I think this conversation has more to do with countermeasures than risk. I'm wondering whether we might could get Joy's team to just come up with some examples that would map to 800-63 risk profiles, some healthcare examples to bring back to this team so that, you know, to get a better understanding what that scale is? I mean y-you have a team, Joy. Are—is that something that you could have them do?

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Yeah. We could probably have, have them do that.

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

You know this, this kind of continuum of—and then bring it back to us.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Although I will, I will say that 800-63 just treats health informa—you know I, I don't know that 800-63 is granular enough really to get you what you're looking for, but we can certainly look at it.

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

Yeah.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

And what we can also do if it would be helpful is to just have a—give you a, a short summary of what the ID-proofing mechanisms—I'm sorry, the authentication mechanisms—that are appropriate for the various levels are now.

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

And ID proofing.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Yeah. Well, just summarizing it from—not ID proofing. Just summarizing it from 800-63 what are the, the ways of authentication for two-factor that are acceptable.

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

Yeah. But 63 also addresses identity proofing, and I think that we, we, we talk—it's difficult to have that discussion about whether, for example, hospitals actually do Level 3 identity proofing without, you know, ha-having it in front of you what it actually calls for.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Okay.

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

But I think, I think your—having your team help us here would be a really good use of them.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Another possible resource is there was a physician committee that's involved with the NSTIC work. I think we heard from one of them in the panel.

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

Oh.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

They probably—they may have done some of this assessment already.

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

Oh, so we could ask Jerry ...?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Probably was—was it David Hunt? Is that the name? Um—

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

There is a David Hunt, and he is with ONC.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Oh, okay.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

And, and he's also a surgeon.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. I'm looking at my notes here. I—we heard from someone who was—who has a physician committee that was associated with the NSTIC work.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Yes. I think he's part of that. I'm not positive, but I think that sounds right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yep. There may be—they may have done some thinking.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

So if you don't—well, what, um, what is our timeline here today? We are on 'til 12?

Deven McGraw – Center for Democracy & Technology – Director

Twelve.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Yes. I would say I could probably pull this, the, the two-factor and the ID-proofing requirements. I can pull that right now. , I'll just get off the phone for a few minutes, and I can send you that while you're having this conversation if you think you have time to deal with it today. If not, we can just hold off on it.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I, I think that, you know, more of an issue is just understanding what we think these risk levels are. It, it—

Deven McGraw – Center for Democracy & Technology – Director

You mean, you mean what constitutes a higher risk transaction in healthcare? Yeah.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. Yeah. And, and, and then, you know, mapping appropriate ac—, you know, I'll call them interventions, if you would—onto those risk categories is where you raise the question of cost and workflow impact and, and you do your tradeoffs between risk and benefit. And you may say in certain cases the risk is higher, but it's just too costly to address it, um, in which case you, you know, you back down to a lower level.

It would be interesting to hear about—from Mark Frisse and their experience with two-factor across the board. I would—I'll be sure to follow up personally if we don't ever—if we don't have any more specific follow-up, 'cause I honestly thought that we were headed to two-factor for everything but obviously I misheard Farzad's emphasis.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Well, um, I, I think for the time being that, that the, the focus—I, I'm not sure that you're wrong, David, eventually. Um, I think that it has not really been explored to the degree of the remote, and that's why I was very careful when I answered your question earlier, which is it's on the table is the way I would put it for everything. But in particular what we want to address most now is this remote access, um, because if you, um—you know, we continue to see from the, the breach notifications that, you know, remote access (remote devices anyways) continue to be problematic.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. No, I, I noticed your careful language.

Deven McGraw – Center for Democracy & Technology – Director

I mean one, one thing that does occur to you is if you've got, you know, a need to sort of credential at a higher level for, you know, use—for certain riskier use cases that are fairly common, at what point do you just—do you just do that as a matter of course, and then you end up using that credential for lower risk transactions 'cause you have it?

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Yeah. Well, that's what NIST is all ab—, NSTIC is all about.

Deven McGraw – Center for Democracy & Technology – Director

Yeah. So speaking—I mean speaking of NSTIC, you know, one of the things I—um, can I, can I get the folks from Altarum to restore my, um, screen control? I, I lost power for a second and when it—when I got—when I logged back in online I didn't have it anymore. Thank you.

Um, you know, we were talking about, you know, sort of do, do you leverage NSTIC to help you get to, um, you know, a scenario where, where individuals within the healthcare system could have Level 3, um, credentials? Um, or, or is it, you know, do we need a more focused healthcare-specific process that's either with-within NSTIC or external to NSTIC? I, you know, I, I just wasn't sure what, what we wanted to say.

We certainly heard from some of the folks at the hearing that, you know, especially our private sector panels that said, "Look, you know, they're—we're committed to making this NSTIC process work for, you know, individuals being, you know, being, um, authenticated across the Internet and, and it, it, you know, it's a process that could work for healthcare as well," was the impression that I got. I, I don't know what, if anything, we want to say in terms of a recommendation before the Policy Committee on this issue.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I, I mean what I—this is David—what I, I heard was, you know, careful language from NSTIC about the emergence of identity ecosystems where you could envision interoperability and trust within the ecosystem and eventually across ecosystems. But there would, there—I think they have a recognition that the, the, the, you know, ecosystems are not going to—they're going to struggle to trust within themselves first and then to trust across.

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

So I, I think, you know, sort of being informed by progress towards widespread interoperability as envisioned by NSTIC makes sense, but I don't think it's reasonable to think that we're going to see healthcare just jump wholeheartedly into a consumer faith in commercial NSTIC world and, and consider that adequate for trust.

It's just so hard in healthcare. I mean, you know, just so many questions will come up—one of which, of course, is, you know, what kind of assertions about the individual are carried forward with their credentials, and healthcare is going to have a very different set of assertions they care about than movie theatres. You know they love to do the, "Are you over 17," example for movie theatres. Well, you know, in healthcare that's not that interesting a question.

Deven McGraw – Center for Democracy & Technology – Director

Right. Okay. That makes sense.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

So I—and I think it's just it bears watching. But I, I think there's going to be more, more than one fob in your pocket for a while, which is sad, sad to say but, um, I just can't imagine that we're going to get past that quickly.

I will, you know, take this radio silence to change the subject. Um, this, this is a little—this is beyond the scope of our current call, but I think it's something that warrants, you know, perhaps some more standards work in the future, and that is back to the notion of capturing some assertions about an individual who had been identity proofed such that those assertions can be cryptographically bound to their identity such that downstream systems can test some of those assertions.

Um, you know, you can imagine a break-the-glass system that says, “You must assert to me that you are in fact a licensed practitioner, um, before I will let you break the glass.” And you could do that via assertions that are bound to identity proofing. I don’t think healthcare has a standard for doing that yet and that may be something that bears, you know, future attention.

Deven McGraw – Center for Democracy & Technology – Director

Yeah. Well, I, I remember when you, when you, you’ve mentioned this in previous conversations, David, and it occurs to me that it’s, that it’s, it, it helps with authentication, but it also helps with some of these access questions that, that we’ve tried to decouple, um, from identity and authentication in our conversations but that are inev-, an inevitable piece of, of the access question is your ability to make certain assertions in certain circumstances.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. Assertions that are bound to your identity could be captured at proofing and cryptographically proven, and that’s valuable if we can agree on what those assertions are.

Deven McGraw – Center for Democracy & Technology – Director

Right. Well, and it also feels like that, that’s such a big conversation that it—or is it enough to say at sort of early stages of, of, of creating an identity ecosystem that you—that there’d be room for a, you know, a mechanism for binding, um, assertions to, to, to identity as opposed to trying to solve all of that at once.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. I, I don’t think it’s a short-term goal.

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

I think we, we, we—today we capture those assertions in the authentication—I’m sorry, in the authorization system—and we match your identity, and then we look you up in an authorization system and say, “You have—you know you are a provider; you can do this. You’re a nurse; you can do that.”

Um, but, some of those assertions (the ones that are bound to your identity) could be moved upstream in an NSTIC future and leveraged by many different relying parties as opposed to each relying party having to capture those assertions independently, which is the world today, which is not going to change in a hurry.

Deven McGraw – Center for Democracy & Technology – Director

Right. Anybody else have any other thoughts on this? So, so just to sort of sum it up, um, we’re going to be very clear with the Policy Committee what set of issues we’re focusing on: identity and authentication of providers in order to enable trusted exchange to meet meaningful use. So that’s the set of transactions. We’re recommending the movement to individual Level of Assurance 3, um, for the set of sort of what we perceive to be riskier exchange transactions, um, that we, we believe needs further defining, but we can come up with some at least initial examples.

Um, we, I believe are still going to ask the Standards Committee for some help, but obviously we want some practicing physician input on that. And at the end of the day, um, the, the risks should be assessed both with respect to security as well as quality of care and, and safety, and that the movement to Level 3, um, could be one involving, , an intermediate sort of 2.5 step where the identity proofing, um, , is still organization driven and not necessarily required to meet, um, the NIST 800-63 standards, but the level of authentication would be, would be two-factor per NIST 800-63. Does that sound about like where we landed?

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

I think I delegated the Privacy and Security Workgroup assignment over to Joy.

Deven McGraw – Center for Democracy & Technology – Director

Oh, okay. You bought yourself out of some work.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

You know there—I, as we've been speaking, I've been going through the 800-63-1 document and a lot of discussions that were posed today are, I think, addressed in that document.

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

I think so too.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

So what we will do is, we will identify—it's a rather—in the terms of standards, it's probably a short document, but for the rest of us it's still a lengthy document. It's about 120 pages.

Deven McGraw – Center for Democracy & Technology – Director

Yes.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

But we will identify the pertinent parts and, and either copy them or PDF them and make notes, circulate them to the group.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

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

And come up with, um, you know, if, if your team can, can come up with healthcare examples for each of those risk levels, that would be really helpful.

Leslie Francis – National Committee on Vital and Health Statistics

This is Leslie. Why not just comment about that when you use the term provider in the first, you know, bullet? Of course, that suggests that they're going to be folks with licenses.

Deven McGraw – Center for Democracy & Technology – Director

Yeah. But, but we're not—I mean, again, it's an identity and authentication issue that we—

Leslie Francis – National Committee on Vital and Health Statistics

Exactly but you need to say it's for anyone.

Deven McGraw – Center for Democracy & Technology – Director

Yeah. It's for users, right.

Leslie Francis – National Committee on Vital and Health Statistics

For users, yeah.

Deven McGraw – Center for Democracy & Technology – Director

Individual—humans, human individual users.

Leslie Francis – National Committee on Vital and Health Statistics

Yep. Right. Right. But I—so I didn't want it to look as though provider meant a narrower group.

Deven McGraw – Center for Democracy & Technology – Director

Yes. A fair point, Leslie. Thank you.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

So just—this is Joy. Just to clarify, when you're looking for the healthcare example for risk profiles, you're looking for us to say, "What's the difference—why, why is remote assess 'riskier' than in the physical facility access." Is that the kind of thing you're looking for?

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

It still goes back to the use cases discussion, last meeting, discussion the last time we met.

Deven McGraw – Center for Democracy & Technology – Director

What do you mean, John?

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

Well, about what, what are the different uses cases and how do they—how does this all apply?

Deven McGraw – Center for Democracy & Technology – Director

But I thought that's the discussion we were having, focusing on remote access and trying to further drill down on what remote means?

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

Well, right but I think—, but I, I agree with that. I'm just saying though that the nuances of what we're talking about here are all—have all been flushed out in the, the some of the, the different use cases that we were also talking about. And that—it's—it is, it is sort of a amalgamation of everything we're talking about is, is we're fleshing out the different sort of—sort of different scenarios under which this occurs.

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

I think we translated that into this continuum of risk that we're asking Joy's group to try to help us.

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

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. Some broad, broad, broad categories and then some examples for each of those categories that would be, you know, concrete, finite subset of the full set of use cases.

Judy Faulkner – Epic Systems – Founder

And, and this is Judy. I'd like to ask about—and I might be confused on this Tier B versus Tier C. Tier B would be multifactor authentication, as I understand it. Tier C is, is NIST, which is an ex-, added expense as I understand it. Um—

Deven McGraw – Center for Democracy & Technology – Director

NIST does not credential people. Judy.

Judy Faulkner – Epic Systems – Founder

I know. I'm sorry. It's NIST that if you—that you have to get the credential from an authorized place.

Deven McGraw – Center for Democracy & Technology – Director

No, that's not what we meant.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

No. They have to follow, follow the rules.

Judy Faulkner – Epic Systems – Founder

Well, what's the difference then between NIST—we, I must have a misunderstanding here. How do you—are those credentials free to get them?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

It, it—

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

It doesn't address that at all.

Deven McGraw – Center for Democracy & Technology – Director

There's not—

David McCallie – Cerner Corporation – Vice President of Medical Informatics

NIST set—this is David—NIST sets the rules that a credentialing iss—a credential-issuing organization would follow.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Judy Faulkner – Epic Systems – Founder

Okay. So when you go to that, isn't there an expense with that, or no?

Deven McGraw – Center for Democracy & Technology – Director

...we haven't gotten to that.

Judy Faulkner – Epic Systems – Founder

Oh, okay. But if in fact you require NIST, then don't you require that?

Deven McGraw – Center for Democracy & Technology – Director

No, not necessarily.

Judy Faulkner – Epic Systems – Founder

Okay. So how do you do NIST without doing NIST certification?

Deven McGraw – Center for Democracy & Technology – Director

NIST, NIST is, NIST is a level—in other words, it sets a standard for your own credentialing.

Judy Faulkner – Epic Systems – Founder

Okay. So, so the organization itself can credential and doesn't have to use the NIST authorizing body?

Deven McGraw – Center for Democracy & Technology – Director

Yeah, doesn't have to be FICAM necessarily or Federal Bridge third person, although certainly there's value for federal exchange in, in having a certificate that's blessed by those organizations.

Judy Faulkner – Epic Systems – Founder

Okay.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yes. So there are—I mean, I think Judy's right that there could be costs when you start bringing the FICAM question to the table, which is we haven't addressed today. That's a step beyond specific NIST credence—standards—

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

—that says that you have to get it from specific approved organizations.

Deven McGraw – Center for Democracy & Technology – Director

I mean the fact is that if you do have Level 3 credentialing of your users you—if you wanted to be a, you know, FICAM certified or accredited, whatever is their appropriate term, y-you, you'd be on the right path to getting there, but we're not saying that that's a requirement.

Judy Faulkner – Epic Systems – Founder

Okay. That's nice to have clarified.

Deven McGraw – Center for Democracy & Technology – Director

Yep. Yeah and the real difference between Tiers B and C—and I went back to that slide—is, um, you know, what, what standards within NIST do you need to satisfy? Is it just on identity proofing or is it both for identity proofing and tokens for authentication? Tier C is the whole enchilada, and tier B is you can identity proof in the way you customarily have, but you've got to use the, the two-factor—you know, you've got to have two-factors that, that are accept, you know, identified in NIST 800-63.

That makes you LOA 3, right? That's the difference. It's—that's why it' staged. But, but I think it will be helpful to sort of lay out in, in a summary form what the difference—you know, what, what's acceptable for both the identity proofing as well as, um, the tokens for authentication for Level of Assurance 3 so people have a full understanding.

And I can commit as, as I write this up in preparation for next Wednesday's meeting I will—I'll get it out to folks and you can, you can give me comments on it to make sure that I, that I hit it right. I think it'll be a more streamlined set of recommendations, but that's always easier to present to the Policy Committee, quite frankly. And I think I'm only going to have 45 minutes, so.

So, Joy, are you comfortable with the assignment that we gave you?

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Well, I understand two parts of it.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

The last one, I'll tell you, I'm still having, a little difficult time wrapping my head around, exactly what you're looking for. And if you could give me some examples it might be helpful because what I said is it, is it basically you want a continuum of risk and healthcare examples of the continuum of risk. Like, what's riskier than other things?

Um, I-I will tell you having looked at this NIST document it just—it, it is much broader than the way we're talking about this, and to the extent that you have the potential of putting at risk identifiable health information that—you know, the fact that it's identifiable health information probably alone would put it in a specific category of risk by the way they look at things.

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

So they don't do the subdivision that you're requesting. And, and we can do that. I'm just, um, letting you know that you will—what you're looking for may not be exactly—what you get may not be exactly what you were looking for.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

But I, but—

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

... I'm sorry.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

This is David, Joy. I mean, I think that, you know, again, that's the sort of the problem with that NIST approach is it, it, it is a one-size fits all, and we've—I mean when you say Level 3, you meet Level 3 across the board.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

And we're saying in healthcare we think that would be disruptive, expensive, and overkill (at least in the near term) and that we would recommend a more fine-grained approach where we would carve out certain cases where we think the risk is low enough that you don't need full Level 3, such as inside the hospital, under observation with directly wired terminals. On the other hand there is—

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Okay. That's exactly where I thought. Okay. So we were on the same page it's above, —

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah. Yeah.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

—and, but, and you're not necessarily tying it to this, so it is like the remote access versus the physical facility.

Deven McGraw – Center for Democracy & Technology – Director

Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yeah.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Got it. Okay.

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

Yeah. But I would—I would, um—and, and it is only authentication risk it's not like, you know, the risk of leaving, you know, other disclosures of health information. It really is, you know, the, um, circumstances under which one is authenticating him, him or herself. But the other thing is that, you know, to give you an example—and I, I would map it to, you know, there are three levels there of assurance in, um, in the NIST 800-63 and I would, I would like to see it mapped because, for example, earlier I raised the man-in-the-middle attack and how Level 3 is not designed to counter man-in-the-middle attacks. And people don't know what that is. So—

Deven McGraw – Center for Democracy & Technology – Director

But that's— ... to me is something that the Standards Committee should do.

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

Um, if, if you really lay out the risk it would make—in, in human terms it, um, you know, give an example of what would be a Level 3, I think that, , I think Joy’s team is, is fine at doing that. You know, they don’t have to describe technically how a man-in-the-middle attack happens, but, you know, they could say, “Well, it’s a fishing kind of a thing,” or “It’s a website that pretends to be somebody it’s not,” you know.

Um, but I think that those examples would help people understand, you know, the level of comfort, if you will, rather than assurance that one would get from a Level 2 authentication versus a Level 3 within a healthcare context.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Well, um, there is—hmmm—

Deven McGraw – Center for Democracy & Technology – Director

I actually think that that’s something that would be relatively easy, Joy, for me to include in the slides as a baseline, because, Dixie, if, if nothing else I can—I could just borrow from the ones that you presented to the Standards Committee so people understand what kind of risk we’re talking about here. To me, I think it’s far more important for us to use the valuable resources of Joy’s team to help us drill down a little bit more on what in healthcare we think is, um—raises those risks more in terms of sort of remote, you know, w-wireless external access. You know the sort of, , brainstorming that we did a little bit of on this call but didn’t necessarily, you know, dive down into, you know—we didn’t come up with a lot of examples, but

I do think it’s helpful for the industry if you’re going to come up with a recommendation that says, you know, you’re going to aim at NIST LOA 3 credentials for, you know, a certain class of, of, of perceived riskier transactions in healthcare with risk defined as risk to, um, trusted identity in cyberspace. Like, you know, what exactly does that mean? Or, or what with some more specificity. Maybe, maybe getting to exactness is asking for too much.

Did that make sense? Is anybody still there?

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Yeah. I’m thinking.

Deven McGraw – Center for Democracy & Technology – Director

Okay. Still thinking?

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Well, I’m trying to figure out what—um, well—

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

... still breathing?

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

I didn’t know you were waiting for me to respond. Did you want a—do you want me—I mean, I guess—

Deven McGraw – Center for Democracy & Technology – Director

I just, I—in other words, I laid out a plan that, that, that I thought addressed Dixie’s desire to make sure that the Policy Committee understands what kind of risk we’re talking about here.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Right. So I was waiting for Dixie to say yes she’d do it.

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

I was waiting for you to say yes you’d do it.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

No. We could have had a long

Deven McGraw – Center for Democracy & Technology – Director

No. I offered to—

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

I like your idea, Deven.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, utilize some of the slides that Dixie used in her presentation to the Standards Committee last week to lay a more, a more, um—, a better foundation for the Policy Committee about just what risks the NIST document aims to address.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Okay.

Deven McGraw – Center for Democracy & Technology – Director

And, and what we would be looking for you to deal with is what we, um—you know, your, your initial right conclusion about sort of the scenarios.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Yeah. So it's the, the continuum of risk ranging from, you know, you're inside a locked sealed room with, with your, your—

Deven McGraw – Center for Democracy & Technology – Director

With somebody else.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Right, just talking to them. No.

Deven McGraw – Center for Democracy & Technology – Director

No. I mean I, you know, again, if we're focusing on, on, on trusted-identity risk, right, and what does that mean in the context of sort of internal access versus remote access across a network, and what are the— what do we mean when we say that, remote access across the network.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Yep. Got it.

Deven McGraw – Center for Democracy & Technology – Director

Everybody else okay?

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Yep.

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

Yeah.

Deven McGraw – Center for Democracy & Technology – Director

Okay. Alright, I think folks are tired. We, we moved from 90 minute calls to two hours and I'm feeling it. Um, does, does anybody have anything else to add? Again, we'll write this up and, and circulate it by e-mail, um—

W

...

Deven McGraw – Center for Democracy & Technology – Director

—this week for folks to look at. Before we open the lines for public comment, does anybody have anything else they would like to add?

W

No.

Deven McGraw – Center for Democracy & Technology – Director

Alright, great. Thanks, thanks for your patients, everyone. This is a tough set of issues. MacKenzie, can you open up the line for public comment?

MacKenzie Robertson – Office of the National Coordinator

Sure thing. Operator, could you please open the lines?

Public Comment

Operator

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

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Great.

Deven McGraw – Center for Democracy & Technology – Director

Thank you, everybody.

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

Hey, thanks, Deven.

Deven McGraw – Center for Democracy & Technology – Director

All right. Talk to you soon.

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

Bye.

Deven McGraw – Center for Democracy & Technology – Director

Look for your e-mails.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Thanks, everyone.

W

Bye.