

HIT Privacy & Security Tiger Team
Draft Transcript
November 15, 2011

Operator

Ms. Deering all lines are bridged.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Thank you Operator. This is Mary Jo Deering in the Office of the National Coordinator for Health Information Technology. This is a public meeting of the Health IT Policy Committee's Privacy and Security Tiger Team. It is a public meeting. There will be a transcript made and there will be an opportunity for comments at the end. I would ask Workgroup members to identify themselves when they speak. I'll take the roll. Deven McGraw?

Deven McGraw – Center for Democracy & Technology – Director

Here.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Paul Egerman?

Paul Egerman – Businessman/Entrepreneur

Here.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Dixie Baker?

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

I'm here.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Christine Bechtel?

Alice Leiter – National Partnership for Women & Families

This is Alice Leiter, I'm here.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Rachel Block? Neil Calman?

Neil Calman – The Institute for Family Health – President and Cofounder

Here.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Carol Diamond?

Rebecca Rockwood – Markle Foundation

This is Rebecca Rockwood I'm joining for Carol.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Judy Faulkner? Gayle Harrell? John Houston?

John Houston – University of Pittsburgh Medical Center – NCVHS

Here.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

David Lansky? David McCallie? Wes Rishel? Micky Tripathi? Latanya Sweeney? And have I missed anyone, a member of the Tiger Team?

Deven McGraw – Center for Democracy & Technology – Director

We have the person from Social Security, should be on the list, I'm blanking on his name, and we always have a representative from the Office of Civil Rights, Verne Rinker.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Fern, F-E-R-N?

Deven McGraw – Center for Democracy & Technology – Director

Verne.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Oh, Verne, okay I'll find that. All right thank you. And also on the line I believe we have Deborah Lafky of ONC?

Deborah Lafky – Office of the Chief Privacy Officer

Here.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

And Kevin Stine?

Kevin Stine – National Institute of Standards and Technology

Here.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Okay. Thank you. Take it away chairs.

Deven McGraw – Center for Democracy & Technology – Director

Okay. Thank you Mary Jo I appreciate it.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Deven it's David McCallie joining late.

Deven McGraw – Center for Democracy & Technology – Director

Oh, great. Thanks David. Glad you could make it.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Thanks.

Micky Tripathi – Massachusetts eHealth Collaborative

Deven, hi, it's Micky Tripathi.

Deven McGraw – Center for Democracy & Technology – Director

Oh, hey Micky, great. All right, so what we're going to talk about today is we actually have a 90 minute call today, which is shorter than our usual two hours, but I'm confident that we can actually get through this material. Most of the call today is going to involve a presentation by Deborah Lafky and Kevin Stine of an analysis that they have done which compares the HIPAA security rule, which covers electronic protected health information, to other commonly used security frameworks and so they will really take the first chunk of the meeting to go through some slides on that analysis. And then Paul and I will chime back in on sort of what our initial conclusions were having had a version of this presentation already on an earlier co-chair call, and then based on those preliminary conclusions we drew up some draft straw recommendations, but those are obviously up for discussion by the Tiger Team as they always are, but we like to put something in front of you to get the conversation started. So that's essentially the agenda for today. I want to thank you all for joining us. And also, as always, thank the members of the public who are listening in. Paul, do you have anything to add before we turn it over to Deborah and Kevin?

Paul Egerman – Businessman/Entrepreneur

No. I think you did a very good summary Deven. The only observation I would make is, you know, we're a Privacy and Security Tiger Team and a lot of people don't make a distinction between privacy and security but this discussion today is really about security.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Paul Egerman – Businessman/Entrepreneur

And it's a very interesting discussion.

Deven McGraw – Center for Democracy & Technology – Director

That's right and security policy, not the technical, not the specific technical standards which of course is in the purview of the Standards Committee and they have their own Privacy and Security Working Group which Dixie Baker Chairs. So with that I want to turn it over to Deborah and Kevin, ask the folks from Altarum to bring up the slides so they can start going through them. Take it away. I don't know which one of you is starting but you can go ahead.

Deborah Lafky – Office of the Chief Privacy Officer

This is Deborah, I'll start. This is Deborah Lafky from the Office of the Chief Privacy Officer and I just wanted to, before I turn it over to Kevin, to take you through the technical analysis, give you some background as to what the goal was here and how we undertook this work. The Office for Civil Rights is responsible for enforcing the HIPAA security rule. The security rule was first promulgated in 2002 and the security rule, if we could go to the next slide please, okay the security rule is essentially a security framework. It provides policies and it provides a set of actions that are associated with those policies and as such it bears many similarities to security frameworks in general. In the world of security right now we have some very strong frameworks such as that associated with the Federal Information Systems Management Act or FISMA, which is a fully fledged security framework that has a number of different domains to it that Kevin is going to describe and it's a very modern and flexible framework, and Kevin Stine is actually from NIST, and he played an important role in producing and publishing the NIST guidance around the FISMA security framework in the form of special publication 800-53.

So, in addition to that security framework, there are other very modern robust security frameworks including one published by the International Standards Organization or ISO, its ISO 27001, often referred to as ISO 27K, and it bears a great deal of similarity to the FISMA framework. One of the issues that we are looking at with the HIPAA security rule is its evolution from where it was when it first came out to where other frameworks are today. During the late 1990s, the security frameworks went through quite rapid evolution and reached a level of maturity that they've pretty much stabilized at today. But the way that this has happened has been through a systematic review process where security frameworks are evaluated and updated periodically through standard setting bodies and other mechanisms. The HIPAA security rule on the other hand has stayed the same since it was first published and this is, I mean, for more than one reason, but one of the reasons is that it can be difficult to revise a regulation once it has been promulgated.

So one of the questions that we sought to address in this work was to look at the HIPAA security rule and compare it to these modern frameworks and suggest or to identify and possibly suggest areas where it could be, where something could be done to improve or increase the alignment of the security rule with these more modern frameworks and as you'll see, as Kevin goes through the slides, you'll see where some of these differences are and you'll see some discussion about what the implications of those differences are, and then at the end you'll see some straw recommendations from Deven and Paul in response to the briefing that we provided with them on this subject earlier. And with that, you know, I wanted to speak briefly to this slide that explains what security frameworks are. They are basically..., they consist of a logically related group of families of security controls, and they may be open standards, and they maybe proprietary.

FISMA is an open standard, ISO is something that you have to purchase, although it's developed in a transparent manner and there are others, which again can be open or proprietary. Basically the bottom line is that the HIPAA security rule has not had a chance to evolve and so this is the subject that we want to address today is whether, when, how, the security rule could possibly be evolved to reach a level of maturity that these other frameworks have reached. With that I am going to turn it over to Kevin and we can go to the next slide.

Kevin Stine – National Institute of Standards and Technology

Great, thank you Deborah. So again, this is Kevin Stine from NIST, I've been supporting ONC on this task, on this analysis. So as Deborah mentioned there are a variety of different security frameworks that exist today. Obviously, the HIPAA security rule being one of them specific to the health care setting and electronic protected health information, certainly ISO, again as Deborah mentioned, an international standard, FISMA, Federal Information Security Management Act as it relates to federal information and information systems, and others as well, the payment card industries, data security standard, CoBIT and then you may be familiar with HITRUST as kind of this framework of frameworks if you will, or, you know, harmonization of the security requirements of existing standards and regulations. If you could go to the next slide please. Can we advance the slide to the next one? Thank you.

So for purposes of this presentation we decided to focus on two of those frameworks one being FISMA and the other being ISO 27001. So FISMA is actually a law. I think, commonly when organizations or when people talk about security frameworks, when they say FISMA they're really referring to some of the bits and pieces, some of the underlying standards and guidelines that NIST has developed in response to our requirements or our responsibilities under FISMA and we'll talk a little bit about those as we move forward through the presentation.

But FISMA is a law, it's a part of the E-Government Act of 2002 and it essentially calls on federal agencies or organizations operating on behalf of federal agencies to protect federal information and information systems and it calls on a variety of different federal agencies from the office of management and budget to NIST to the agency heads of each of the departments and agencies to establish information security programs and implement those programs to provide for the security so the confidentiality, integrity, and availability of information and information systems in support of federal activities. And ISO 27001 is Information Security Management system requirements. Where it is similar to FISMA, you know, looking at specifying requirements within the context of overall business risk. If we could advance to the next slide, please.

So FISMA tasked NIST to do a number of things, one of those things was to develop standards and guidelines that can assist federal agencies in providing adequate information security for their operations and assets. So we're really looking at providing information security for federal information and information systems. Again, as I mentioned on the previous slide, FISMA is a law and again some of the underlying standards and guidelines we were asked to develop and issue under our responsibilities or our tasking in FISMA were in the form of Federal Information Processing Standards or FIPS and special publications which are really the guidelines that NIST issues. You may be familiar with the 800-series of special publications which are kind of the information security family of publications and resources that we issue at NIST.

So, Federal Information Processing Standard 200 or FIPS 200 provides a very high level discussion of security related areas, minimum requirements for federal agencies to implement. So, being a standard it is mandatory for federal agency use. It is certainly voluntarily adopted much like many of other standards, it is voluntarily adopted frequently by other sectors, by other types of organizations that do not fall within the scope of FISMA or under the FISMA umbrella. In support of FIPS 200, which is again, written at a fairly high level of abstraction defining just 17 security related areas that agencies need to implement to protect information and information systems, we also issued what many of you may know about is special publication 800-53, which is a companion guide, if you will, to FIPS 200. So, 800-53 provides a consistent repeatable process for helping agencies and organizations to select, specify and then implement information security controls to protect their information and information systems. Most people know 800-53 because in one of the appendices it provides a fairly comprehensive catalog of security controls across the 17 security control families that were specified in FIPS 200.

And as we advance to the next slide, the next slide talks about what those 17 control families are. So the control families are essentially, you know, higher level groupings of security controls across a variety of different security functional or security capability areas. Some of those range from, you know, they range from the management, the operational, to the technical security controls. For example, access control, audit and accountability, awareness and training, you know, the list goes on and on. You'll see 17 there and those 17 bulleted items are the same 17 families that are called or 17 security related areas that are called out in FIPS 200. So, when we talk about 800-53, 800-53 takes these 17 control families and breaks them down into a collection of security controls that are most appropriate or most relevant to those particular functional areas and provides a more granular level of information to assist organizations with, you know, having a better understanding of the security objective of the family and of the particular control that you're talking about and then provides implementation guidelines or implementation guidance and supplemental guidance that can help organizations to better implement that control within their organization as well as some other considerations that agencies and other organizations may consider as they're moving forward with their implementation.

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

This is Dixie, Deven do you want questions as we go or do you want us to save them to the end?

Deven McGraw – Center for Democracy & Technology – Director

I think if you have, Kevin, I don't know if you have a preference?

Kevin Stine – National Institute of Standards and Technology

I'm certainly fine taking questions as we go and I'd look to Deven or Paul if you would like us to move forward due to time.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, let's try with questions during and if that turns out to slow us down too much we'll default to at the end. So go ahead Dixie.

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

Okay. So my only question is when you accredit, whoever is the accreditor, when an accreditor accredits a federal system, do they accredit it against the FISMA law, the FIPS 200 SP 800-53 or something else?

Kevin Stine – National Institute of Standards and Technology

So, when an authorizing official authorizes a system to operate or to use your words, to accredit a system to operate, they're accrediting that system based on the security controls that have been selected and implemented for that system or for that agency and those security controls come from Special Publication 800-53. Does that answer your question Dixie?

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

So you look to see that 800-53 tells you how that particular security control should be implemented so you develop a test script against that right?

Kevin Stine – National Institute of Standards and Technology

In a nutshell, yes. Now we do have a companion guideline to the control catalog in 800-53. The companion guide is called 800-53a and that provides detailed assessment procedures for all of the controls in the control catalog. So, as an organization selects their controls from 800-53 catalog they develop their assessment plan using the procedures that we've developed in 800-53a and then the results of the assessment, of the controls that have been implemented, in part supports the decision to accredit the information system.

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

Okay. Thank you.

Kevin Stine – National Institute of Standards and Technology

Sure. So FIPS 200 was issued I think back in 2006 and obviously security and technologies don't stand still. So the original 17 control families that were specified in FIPS 200 are still relevant, but obviously there are new families that we look to add periodically. There is a little bulleted footnote at the bottom there that specifies two additional control families that one has been added in the most recent final version of 800-53 looking at security program management controls. So these higher level organization wide security controls and functions that should be in place, such as identifying an information security officer for your organization, integrating security into your enterprise architecture, into your capital planning and budget control processes and things like that. So looking at security from a program perspective. So that's a new family that's been added in one of the appendices to 800-53. Another one that's out actually that has been out for public comment that will be added in the next revision to 800-53, which will be revision 4, is a family looking at privacy controls for federal information and information systems. And those very closely align with the fair information practices that you may be familiar with as well. So if we could advance to the next slide.

And let me unlock my screen I'm sorry. I want to make sure I'm looking at the same slide. So the next slide gives you an example of one of these security control families on the left and then kind of a snapshot of two of the controls in that family just to give you a better idea of, you know, the format and the structure of some of these items that we've been talking about. So, on the left you'll see the listing of the access control family. So this is the set of security controls that are within that higher level access control family. So, we're walking down through, you know, different layers of abstraction, down, you know, through more granular from the family into the control and then actually you see the little boxes to the right that actually blow out two of these security controls and provide information, you know, provide the control requirements in this case for AC-1, which is access control policy and procedure and then AC-11, which is, as another example, the control requirements for session lock or the control objective for session lock.

So if you scan down that list you'll notice that they're in numerical order and as you get to AC-11 then we skip to AC-14, that's not an oversight. As we go through revisions of these publications, they're always put out for public draft and we receive a lot of public comment and sometimes when we review a collection of public comments, sometimes it makes sense to maybe collapse security controls because there's related functionality, sometimes we withdraw controls for one reason or another, but we don't reuse those control numbers because the control catalog is used heavily, not only by federal agencies but also by tool vendors that build solutions that leverage these control catalogs. So, rather than replace, in this case, you know, AC-12 with a different control, there is a trickledown effect to a much broader audience so we try not to do that. So that provides a snapshot of what we mean when we say a security control family, and then some example of security controls within that family just to kind of level set the discussion here. So if we could advance to next slide, please. So really what, next slide, just waiting for it to.

Deven McGraw – Center for Democracy & Technology – Director

All right, I appear to have the controls Kevin as well. So I'll go ahead and advance them for you.

Kevin Stine – National Institute of Standards and Technology

Okay. Thank you. So, the rest of this presentation is really looking at, you know, so we've said a little bit on security frameworks and dug a little deeper into FISMA and the standards and guidelines in support of FISMA that NIST has issued and a little bit more about those. So the rest of the presentation is going to focus on, you know, this relationship between frameworks and for the purposes of this discussion we are talking about the relationship between FISMA and ISO, and the HIPAA security rule. They certainly all relate, at a high level, when we're talking about the security functional areas such as, you know, the need for access control or the need for security policies and procedures and things like that, but as we drill down through the different frameworks, there is certainly a difference in the level of detail provided that organizations may or may not need to better implement these types of security controls to protect the information that they're entrusted to protect. So if we could advance to next slide.

Deven McGraw – Center for Democracy & Technology – Director

Sure.

Kevin Stine – National Institute of Standards and Technology

Thank you. So here's one example, and we chose risk analysis that seemed to be a pretty important one, certainly at NIST we get a lot of questions from federal agencies about how to do a good risk assessment or a good risk analysis, but as we begin to talk more and more to folks in other sectors, you know, there are requirements for risk analysis in those sectors as well and their framework reflects the importance of that requirement and how to use the results of a risk analysis or a risk assessment to improve your security capabilities to protect the information.

So, in the case of HIPAA, there is a required specification on risk analysis and when you look at 800-53 or ISO 27001, there are clear mappings in relationships between security controls in those two frameworks to the requirements in the HIPAA security rule. Looking at 800-53 for example, there are security controls for risk assessment, for vulnerable scanning, for having a comprehensive risk management strategy, performing a security impact analysis and this is just a snippet of controls that would be most closely related to, again at a high level, to the risk analysis requirements out of the security rule. And ISO, you know, much like FISMA, much like 800-53 has security requirements specified within that framework as well that clearly support the different elements or different objectives that are found within the risk analysis specification. So if we could advance to the next slide. And certainly if there are any questions feel free to chime in.

Deven McGraw – Center for Democracy & Technology – Director

Did I go too far? Yep.

Kevin Stine – National Institute of Standards and Technology

Yeah, back one, so, thank you. So, as I covered on the previous slide, I think, you know, the security rule does specify risk analysis to be done and this is consistent with other security frameworks including the ones that we've discussed here FISMA and ISO. The implication also is that if the risk analysis is performed the system will receive a similar level of risk analysis or risk assessment that you would see across other systems and other frameworks leading to, you know, a more consistent repeatable process and it's a good practice across frameworks as well.

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

Deven, this is Dixie. Do the other, do FISMA and ISO specify frequency?

Deven McGraw – Center for Democracy & Technology – Director

Do you know that Kevin? How often it has to be done, the risk assessment?

Kevin Stine – National Institute of Standards and Technology

So, FISMA provides a, and when I say FISMA I mean 800-53, we try to provide flexibility to organizations, to specify those types of parameters as time based parameters in terms of frequency I believe, but I'd have to go back to the actual control language. I believe risk assessment minimally is at least an annual effort. But really you're doing risk assessment and risk analysis activities all the time through your continuous monitoring of your environments, your infrastructure and your information systems as well.

So, while you can say there's a particular frequency that's been specified, you know, there's certainly risk analysis and risk assessment activities being done on an ongoing basis.

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

Yeah, well the HIMSS surveys have shown that the health care organizations that have responded to their surveys, to be clear, don't do it even annually let alone on a recurring basis.

Kevin Stine – National Institute of Standards and Technology

Sure. Yeah, I think that's usually my understanding or my knowledge of the HIMSS surveys in the past, is that that seems to be a recurring theme year-over-year.

Deven McGraw – Center for Democracy & Technology – Director

Yes.

Leslie Francis – University of Utah School of Medicine

This is Leslie Francis and I've joined late and I apologize, but the worry I always have about risk assessment is unless there's more said about what you're going to end up doing with it, it can just can give people a false sense of security.

Kevin Stine – National Institute of Standards and Technology

So, I...

Deven McGraw – Center for Democracy & Technology – Director

Yeah, so Leslie, I think, you know, the risk assessment is just one piece of a bigger picture.

Leslie Francis – University of Utah School of Medicine

Oh, I know.

Deven McGraw – Center for Democracy & Technology – Director

And we should probably hold off on sort of conclusions until we get to the...

Leslie Francis – University of Utah School of Medicine

Totally fair.

Deven McGraw – Center for Democracy & Technology – Director

Go ahead, Kevin.

Kevin Stine – National Institute of Standards and Technology

Okay. So we're on the right slide. So, we'll look at another example where there may not be that same level of, you know, that same type of relationship between the various frameworks and one area that we identified through our more detailed analysis is one in boundary protections. So, there are very explicit security controls in 800-53 with respect to boundary protections and when I say boundary protections I'm talking about not only kind of your organizations network perimeter boundary protections like your firewalls and your routers and things like that, but also getting into, within your organization, protecting, you know, your systems or maybe a particular database that maybe slightly more sensitive than others for example due to the type of data that it's holding or processing.

So, protecting those resources not only from external perspectives but also internal perspectives as well, that could be again, you know, internally based firewalls or routers or some sort of, you know, more complex access control lists and things like that. FISMA, the 800-53 controls provide a certain degree of specificity around boundary protections and the types of things that organizations should implement and also should consider during their implementation, and then also how to assess those implementations with respect to what you would expect to see from boundary protections.

ISO has a comparable level of detail, not as much on the implementation side, but there's certainly a lot of security control statements or security requirements specified in ISO 27001 that are supportive of the importance of boundary protections and the need for those at multiple layers within the organization. When we look at those requirements or those security control capabilities in FISMA and in ISO 27001, we don't see the same level of control requirement, the same type of control requirement being called out in the HIPAA security rule. Part of that maybe because just the difference in the discussion, the layer of abstraction, if you will. So HIPAA is written at a much higher level kind of the thou shalt do access control without actually digging into, you know, what that access control actually looks like. Certainly the 800-53 and the ISO provide more specificity in terms of what boundary protections should look like and what organizations should consider. If we could advance to the next slide.

So the implication there is that as organizations move forward with their efforts to implement the requirements of the HIPAA security rule, there may be security functional areas that they're not considering because they're not specified explicitly within the rule and the concern would be that one of those could be boundary protection as an example and boundary safeguards, and following that thread, if you don't have those type of boundary protections in place data could be at risk, you may not be in a position to deter attack or identify attack and then defend against that as well. So that would be a tangible potential impact by not having those types of capabilities in place. Go ahead and advance to the next slide. Back one.

Deven McGraw – Center for Democracy & Technology – Director

All right, the folks from Altarum I have the slides now, thanks.

Caitlin Collins – Altarum Institute

No problem, thanks.

Kevin Stine – National Institute of Standards and Technology

Thank you. So, it's always dangerous to put any kind of numbers out there because they can be sliced and diced, and interpreted in many different ways, so I'll provide you the facts on this table and I'll leave the interpretation of the numbers and the value of the numbers to other folks. So, as part of our analysis of these different frameworks, and this particular table looks specifically at 800-53 and the HIPAA security rule, so the relationship between the two, you'll see in the first column the 17+1 control family, so the 17 control family specified in 5200 and then the program management family as well on the bottom. You'll see the total number of controls in each family and then based on our detailed mapping or analysis of the different framework requirements we mapped security controls in 53 to the different standards and implementation specifications both required and addressable in the HIPAA security rule. And the third column provides the count of the controls in 800-53 that we were able to kind of find a home for in the security rule. So we were able to perform that mapping. And the percentages on the far right column provide, it's the simple math, using the numbers in other two columns.

There are certainly many families where there is, you know, what we would consider 100% coverage where all of the controls within 800-53 are even at a higher level captured within the standards or implementation specifications in the security rule. There are other families, as you can see, I think they're the ones highlighted in yellow where we weren't able to identify a 100% mapping between the controls and the standards and specifications on the other side as well. So I will actually stop there and open up for questions.

Deven McGraw – Center for Democracy & Technology – Director

Why don't we...

Kevin Stine – National Institute of Standards and Technology

If you want to continue Deven.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, thanks Kevin. Thanks very much. Paul and I have some subsequent slides to sort of kick off our discussion including some, you know, sort of initial thoughts that he and I had after viewing this

presentation for the first time, but before we move to that I want to make sure that there aren't any substantive questions that any Tiger Team members have on the call that they want to get addressed before we move into the conclusory phase here.

John Houston – University of Pittsburgh Medical Center – NCVHS

Define substantive.

Deven McGraw – Center for Democracy & Technology – Director

Questions about the gap analysis, questions about the difference between a framework in FISMA and the security rule approach, well either that John or you can just ask your question and we'll see if it fits in the prediscussion question period or should fit within the discussion period.

John Houston – University of Pittsburgh Medical Center – NCVHS

Well, I mean, I have a lot of opinions here.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, no let's stick with questions before opinions.

John Houston – University of Pittsburgh Medical Center – NCVHS

I guess one question that I do have is we've talked about FISMA and one of the things that I know that you can see pursuing is HITECH certification, which is one of the other quasi frameworks which you discussed. Maybe it's part of the discussion, but is there a reason why HITECH is not being discussed versus FISMA or is that just...

Deborah Lafky – Office of the Chief Privacy Officer

This is Deborah, do you mean HITRUST?

John Houston – University of Pittsburgh Medical Center – NCVHS

I'm sorry, HITRUST, I'm sorry, I'm getting, I have too many things on my brain, sorry. HISTRUST, sorry.

Deborah Lafky – Office of the Chief Privacy Officer

Deven, I can respond to that if you'd like?

Deven McGraw – Center for Democracy & Technology – Director

Yeah, absolutely.

Deborah Lafky – Office of the Chief Privacy Officer

The reason that we didn't specifically call out HITRUST is that what HITRUST is, is sort of a meta-framework, it's a synthesis of existing frameworks and they have a document that actually does the crosswalk between FISMA and ISO 27001, and CoBIT, which is another standard and one or two others and in a sense, the gap analysis that we performed does something similar to what HITRUST does, but specifically with respect to the security rule and I also wanted to point out that one of the issues that motivated ONC to look at this question is concern for the small provider who, you know, may not be able to take the 425 pages of the HITRUST common security framework and successfully evaluate themselves against it. So, we are looking for something simpler.

John Houston – University of Pittsburgh Medical Center – NCVHS

Fair enough.

Deven McGraw – Center for Democracy & Technology – Director

Okay, any other questions about this analysis before we move in to the discussion phase where people are free to express their opinions?

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

I have one more, this is Dixie.

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

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

And John's question actually triggered this, is that the HITECH also included some expansions of the HIPAA security rule like, you know, accounting of disclosures which is a type of boundary protection, was that factored in?

Kevin Stine – National Institute of Standards and Technology

This is Kevin. Are you referring to factoring that into the analysis that we did, the mapping?

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

Yes.

Kevin Stine – National Institute of Standards and Technology

No, no that was not.

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

And it's really sort of a weak boundary protection but it's sort of in that ilk, okay, thank you.

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

Verne Rinker – Office for Civil Rights

This is Vern. One question for Kevin or if you wouldn't mind speaking a little bit more on it, with respect to slide 11, you, and I think accurately, said the security rule kind of sets out a more broad brush set of standard and doesn't go very specific, but that some of the NIST standards actually do the more prescriptive. I think the security rule takes that perspective because it's applying across the board. Can you elaborate on the kind of across the board application with having the more specific standards that NIST puts out, my opinion is it's equally problematic on the opposite side, but if you could touch on that I think that would be helpful.

Kevin Stine – National Institute of Standards and Technology

So I want to make sure I understand your question first. So, certainly within the federal space, across the federal government you have a very diverse set of missions, you know, across the different agencies and departments, not only just mission space but also the sizes of federal agencies, you know, from the large cabinet level departments to some very small independent agencies, if you will, things like the National Endowment of the Arts for example or similar type agencies, you know, the same FISMA requirements apply. So the same security controls in 800-53 would be applicable to both a Department of Health and Human Services as well as a smaller micro-agency.

So the broad FISMA framework in terms of the process by which agencies select and implement security controls is very flexible and very tailorable to the constraints of the organization that's implementing them. We provide the catalog as a resource which does specify minimum baselines in support of the higher level standard, but agencies do have maximum flexibility to select controls from the catalog that best provide the security functionality that they need to meet their security objectives.

So there is certainly many of the same challenges as you indicated on the opposite side here, but from our experience with the federal agencies, having that consistent process to follow to select controls and then having a control catalog to select from provides the agencies with that necessary flexibility regardless of their size or mission.

Verne Rinker – Office for Civil Rights

Okay.

Kevin Stine – National Institute of Standards and Technology

Does that help to answer or clarify a little bit?

Verne Rinker – Office for Civil Rights

It does. Does that change at all once you start taking it to a more, to not the federal government but other entities looking to the FISMA standards for their use?

Kevin Stine – National Institute of Standards and Technology

So, I'm sure it could. So FISMA, the law in and of itself, and our standards and guidelines really only apply to the federal agencies or organizations operating on behalf of the federal government. So, they're certainly frequently adopted voluntarily by these organizations and are used in I'm sure a variety of different ways to best meet their needs but more as voluntary resources. So, I don't have a whole lot of information beyond just, you know, a little anecdotal information on how those have been applied and the effectiveness of those within other operating environments.

Verne Rinker – Office for Civil Rights

Okay. Thanks. Yeah, I just wanted to, I think I just want to have the perspective on both sides.

Kevin Stine – National Institute of Standards and Technology

Sure, absolutely.

Deven McGraw – Center for Democracy & Technology – Director

Anybody else before we, you know, one thing that occurs to me, Kevin, and it just occurred to me actually in your explanation to Vern, to his last question, is that, and I want to make sure that I'm drawing the right conclusions, I'm answering my own question, but I want to make sure I'm doing it right.

Kevin Stine – National Institute of Standards and Technology

Sure.

Deven McGraw – Center for Democracy & Technology – Director

So in the HIPAA security rule we know, you know, from our experience as a team, and there's a number of us who are pretty intimately familiar with the security rule, when a implementation specification is addressable, it doesn't mean you can ignore it, but it does give you some flexibility with respect to implementing the sort of general security protection that is sought but having some, you could seek other options if you have reasons for doing so, you know, roughly stating, trying to roughly state the law, but there aren't necessarily sort of a menu of options for you to choose from. It sounds to me like in some of these frameworks where you have, you know, sort of a list of controls that are applicable to a specific security family that you do have some options, you know, that the options are more specified in terms of how you meet the general security protection that is being sought. Is that a safe conclusion? Am I concluding that right in terms of sort of maybe the difference between a framework based approach and the way the security rule tries to implement some flexibility?

Kevin Stine – National Institute of Standards and Technology

Yeah, yeah, I think I would tend to agree with everything you said at least very simply put. There are obviously nuances in everything, but, yes at the highest level, yeah I agree with what you stated, Deven. Let me give you a more concrete example of the type of, just a real brief example of the type of flexibility that agencies have with 800-53 for example. So, when a control says an agency must have a password policy and then the control will call out different elements of that password policy such as password complexity, you know, the agencies must determine what their complexity is, what the number of characters that need to be included in the password things like that, as well as password expiration, so do you have to change it every 90 days or is it 30 days, whatever the case maybe. So, 800-53 and the controls within 53 do not specify those values or those parameters is what we call them. We leave those as what we call organization defined parameters. So, if an organization chooses to implement something at a 30-day password reset, great. If they choose to implement at 90 day password reset that's also great, based on their risk assessment results that may be an appropriate decision for them. So that's the type of flexibility that we see within the framework, within the 53 in the controls.

Deven McGraw – Center for Democracy & Technology – Director

Thanks, that's helpful.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Deven, this is David with a question?

Deven McGraw – Center for Democracy & Technology – Director

Yeah, go ahead.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

It's a vague question and it may border in the direction of our discussion, but I'm curious to know, now that this FISMA and 800-53 have been around for a while, have studies been done to assess the cost effectiveness of this approach? Are there assessments that basically warrant that it be applied across the board? Does it do the job?

Kevin Stine – National Institute of Standards and Technology

So, NIST has not done any assessment of the cost effectiveness of implementing the FIPS 200 and the 800-53 controls, although I'm sure there are plenty of organizations outside the federal government that have done some sort of analysis on their own. What we tried to do is specify the process for selecting security controls. So, having a consistent and repeatable process that agencies can use, so that we're essentially all talking the same risk or trust language if you will. So I know that at HHS you're following the same process that you are following over DOJ for example. So we're all talking the same language here with respect to security and risk. How you implement within your organization, I mean, certainly cost effectiveness, you know, the cost of controls versus, you know, the security benefit that you're receiving from them is certainly a consideration that agencies need to make, but I'm not aware of any NIST analysis of that aspect of it. But the framework certainly provides that level of implementation flexibility so agencies can come up with more creative ways that meet the intent of the security controls if you will.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Okay. Thank you.

Deven McGraw – Center for Democracy & Technology – Director

All right. Thanks a lot to both Kevin and Deborah; I think folks are eager to move into the opinion/recommendation phase of the discussion. When Paul Eggerman and I first got this presentation from Kevin and Deborah in preparation for this meeting we came to the following initial conclusions which is, you know, you just have to look at the comparison table to say, yes there appear to be gaps that exist between the HIPAA security rule and other commonly used security frameworks and certainly that table really focuses on FISMA, but that's not the only one that the team looked at and this was a conclusion that Kevin and Deborah themselves drew earlier in the slide deck.

It also seems like the framework approach that is used in these other context that were explored seems to allow for more frequent updating to keep up innovation maybe that's the distinction between trying to do it all in a Reg and doing it in a combination of regulation and regularly updated guidance, I'm not sure from a format perspective which is better, but we get more frequent updates with these other frameworks and clearly the field is innovating in the space. But we also concluded that a really detailed analysis of the specific gaps and coming up with recommendations that would address specific security areas was likely beyond the expertise of the Policy Committee that we ultimately filter all of our recommendations to and it's arguably beyond the expertise of at least some of us on the Tiger Team, although clearly not all of us.

We also felt that punching this issue to the Standards Committee where there are many more experts on security probably also wasn't appropriate given that there are policy issues that are nested or obvious in these gaps, it's not just about the absence of technical standards or requirements. And so, you know, that really led us to come up with some recommendations that are a bit more over arching and more process oriented than down into the specific details and I want to turn it over to Paul to take us through what we are putting before you but that are completely open for discussion. So, go ahead, Paul.

Paul Egerman – Businessman/Entrepreneur

Yes. Thank you much Deven. This is Paul Egerman. So, exactly as Deven said, is rather than look at the specifics of the frameworks or each specific example that was just presented, what we tried to do was sort of like look at it at more of a higher level and say, well what does this mean in terms of what we call security policy and what security policy recommendations might we make? And so, the two things you see on the screen right now is, the first one it says, you know, security policy needs to be responsive to innovation and changes. So, at least for me, one of the thoughts I got from this presentation is well there's a need to have a way to do security policy that is in some sense dynamic, that you can change from time to time, exactly as Deven said, as a result of, I don't know changing technology, changing environment, new information learned.

And the second bullet also though relates to Deborah Lafky made a comment on, which is the policy needs to be flexible and scalable given the difference in size and resources of the entities. So, you know, we got some questions, say from John Houston at UPMC, I personally am not familiar with UPMC's security policies, but I've seen other similarly large organizations, you know, like Sutter and Kaiser, usually large organizations have very carefully well thought out policies and security experts on their staff and they need that for lots of reasons, one is they have literally thousands, possibly tens of thousands of people interacting with their systems, but on the other end of the spectrum you have, you know, a solo practitioner or a two person, or a three person group practice which has different capabilities in terms of technical capabilities, but possibly a different security environment where for example, in some cases, everybody who works together is known to each other, they work frequently in a single location are even visible to each other and so there may be different security issues related to that environment than the extremely large environment.

So, the two concepts here is, one is dynamic and the second one is sort of a flexibility and scalability to consider the very wide range of environments that we are talking about. So, that was sort of like two concepts that we had and then based on those concepts we had these sort of like draft recommendations which is HHS needs to create some sort of a consistent and more dynamic process for regularly updating the security policies and technical standards. And, you know, basically that's it. And then in using a more dynamic process there might be multiple policy levers that HHS could use, which could include Meaningful Use or it could use other federal funding programs, but the main concept there is consistent more dynamic. And the second concept that we had here was HSS should begin by evaluating this gap analysis in more detail with a goal of closing or maybe a better word might be solving, because you might decide that there are reasons why you don't necessarily want to adopt what the frameworks are doing but resolving the gaps within a reasonable period of time and the question is whether or not we should specify the time.

So, anyway that was our thought as to how to do this from a policy standpoint. And so let me pause and see what people's reactions are if they think it's reasonable, if they have alternatives, if they think we missed something, if it's a bad idea, what do you think?

Leslie Francis – University of Utah School of Medicine

This is Leslie, I think it's absolutely reasonable but I would also add there that there needs to be some kind of minimum so people aren't unfairly surprised when they change concepts because patients aren't going to see the difference or imagine the difference between a small office and UPMC.

Gayle Harrell – Consumer Representative/Florida – Florida State Legislator

This is Gayle Harrell. I got on the conversation very late but I did look at the slides beforehand and I think there needs to be some minimum standard set and with the flexibility built in but you need a floor. People need, the public needs to know that there are some very basic minimum security standards in place. Otherwise, you know, they will become very frightened about the intrusions that can happen and, you know, I think perhaps there needs to be some direction as to what those minimums might be.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, I mean we did Gayle on the previous slide, it does talk in the same bullet where we talk about the need for flexibility, we also say, at the same time, you know, you still need a baseline.

Gayle Harrell – Consumer Representative/Florida – Florida State Legislator

Absolutely.

Deven McGraw – Center for Democracy & Technology – Director

And you need to implement a baseline.

Paul Egerman – Businessman/Entrepreneur

Agreed.

John Houston – University of Pittsburgh Medical Center – NCVHS

Can I ask Paul a question about his last slide?

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

John Houston – University of Pittsburgh Medical Center – NCVHS

When you say we should have dynamic process for regularly updating security policies and technical standards for electronic health records and electronic health information exchange, I hate to ask a simple question, but give me an example a security policy and a technical standard that we are talking about needing to update.

Deven McGraw – Center for Democracy & Technology – Director

Well, I guess we were trying to address the gaps that were identified in the work that Deborah and Kevin did on behalf of ONC but without calling out a specific gap because we thought we just don't have the expertise to dive into the level of detail and say for example, in boundary protections, which was one of the ones that was highlighted, you should do x or y. Instead we're asking for, we're responding to the issue of keeping the set of security policies that apply to electronic health information relevant and more up to date with technology develops versus picking on a specific standard. So...

John Houston – University of Pittsburgh Medical Center – NCVHS

I guess part of my challenge here is what HIPAA says in essence, in my simple interpretation, is that you ultimately, an organization has to adopt reasonable policies based upon their own particular environment and implement appropriate security based upon their own particular environment, and so really in large measure it's up to the covered entity to decide exactly how it has to address each one of the HIPAA requirements itself for security and so it really is up to each individual covered entity to decide which securities policies and technical standards that it thinks it needs to apply. Am I missing something or I am I getting something wrong in the way we're discussing this?

Deven McGraw – Center for Democracy & Technology – Director

So in other words are you arguing, John, that HIPAA already sort of sets sufficient law and policy here and we don't need to do anything more to it is that what you're?

John Houston – University of Pittsburgh Medical Center – NCVHS

Well, I guess for an organization like mine which is committed to complying with HIPAA and having a very secure environment, I like the flexibility of HIPAA because it doesn't tell me what I have to do. It gets out of my way so I can say okay I need to do x, y and z and I have a staff of over 40 people doing information security I'm saying, 40, so, you know, they work constantly looking threat vectors, technologies we deploy, how we deploy them, where we deploy them, and decide, I mean constantly as to what we need to do to ensure that we adequately protect the data and when I see things like FISMA, and I hate to tell you, I sort of cringe when I see the word FISMA, because so many cases when I have to deal with the federal government on certain contracts they'll say you have to comply with FISMA and there's very little granularity as to what that means, there's no detail and so I get concerned when I start to see mention of FISMA. I like my flexibility because I know what I need to do to protect my information.

Paul Egerman – Businessman/Entrepreneur

So those are great comments, John, but I also want to reflect a minute about the comments that both Leslie and Gayle made, which they said the public needs to have a minimum level of security and they both used the word minimum although the slides use the word baseline, and so the issue is still a large organization is able to do what you are able to do, but a smaller organization isn't. And so the question that we're saying is should HHS have a dynamic process to update security policy and technical standards and if you ask for example, an example might be a situation, I'll put in a very broad situation, where, you know, we're starting to see more and more people use the, you know, iPads or tablet computing in health care, and so the question becomes, well does that change anything from a security standpoint? The answer might be no there is no change or the answer might be here is what you need to do as a minimum, or the same might be true of like PDAs, some of you say, well gee, you know, there's a popular device that people use and it's popular but it's also limited in some ways in terms of the capabilities. Do we need to have standards around that?

And so the question becomes do we want HHS to have a mechanism to consider these things and to dynamically respond. If the answer is yes, then I think we can do the minimum that Leslie and Gayle seem to be asking for, the baseline that sort of says, well if you use these things here's, you know, the minimum baseline of what you have to do.

John Houston – University of Pittsburgh Medical Center – NCVHS

But I would also then say that one of my concerns for small providers is going to be if you give them a guidance like FISMA their eyes are going to cross and they're going to take the FISMA standards and they're going to, if they printed them out they're going to throw them on a shelf or in the trash can because it's going to be too much for them to bear.

Paul Egerman – Businessman/Entrepreneur

Well that's true and that's maybe something we've got to be clearer in the recommendations, is that not only is it dynamic, but it's got to be scalable based upon this sort of wide range of organizational settings that it needs to be applied to.

Deven McGraw – Center for Democracy & Technology – Director

Yeah. I think what we're trying to achieve here and maybe it wasn't as clearly stated as it could have been, is to maintain the same premise that the HIPAA security rule was the foundation for the security rule and is also the foundation for some of these other security frameworks, which is you do want a consistent baseline below which no one is allowed to fall, but you also need to have flexibility and scalability with respect to, you know, what you do above and beyond the baseline in terms of the expectations, but having said that, what I think we saw in the analysis that Deborah and Kevin performed was that in terms of sort of mapping what is covered under these other frameworks, and what the security rule covers, there are some deficiencies where there are some gaps in areas that are covered by these other frameworks that are not covered by the security rule and so keeping in mind the sort of model of baseline plus some flexibility and scalability, there ought to be a way to have the security rule be more responsive to innovation in the way that some of these frameworks are, and asking HHS to take a more in depth look at some of the gaps that have been uncovered in this analysis and determine whether and how they could resolve them within some period of time.

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

This is Dixie. First of all, two things, number one, I want to clarify off of what John said, HIPAA is not completely decide which one of these is good for your organization. HIPAA does have a baseline, you know, all of the standards and all of the required implementation specifications have no flexibility, you can't decide, you know, to do it a different way.

John Houston – University of Pittsburgh Medical Center – NCVHS

You're right. I mean you are right.

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

This is a public committee and I want to be clear. My second point, I think that HIPAA does provide a mechanism for responding to changes in technologies that is inherent in its dependency on a risk assessment, because if you really did recurring risk assessment, like Kevin talked about, you would discover that, well, you know, I've got a new risk, I've got wireless around here because my risk assessment tells me that I need to implement counter measures against those vulnerabilities, those list that I've identified. So, I think that HIPAA inherently, because it relies on the risk assessment, inherently has a way to be flexible and to respond to new risks in the environment. So those two are my statements.

My third is a question to Kevin is that we seem to be assuming that FISMA is updated more frequently than HIPAA and I'd be interested in knowing, you know, does having a framework like FISMA, is it updated more frequently than HIPAA?

Kevin Stine – National Institute of Standards and Technology

So, FISMA, the legislation, no. Even FIPS 200 the standard, no, that was issued once in I think 2006 and it was at such a high level it has not been updated since and that's by design. We do revise 800-53 frequently on the scale every other year. So, later, probably second quarter 2012, we'll be issuing revision 4 of 800-53. So, pretty much every two years we'll come out with a revision.

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

Then I would suggest to Paul and Deven that this Tiger Team consider a recommendation that says that we have a guidance that's implemented every two years or something, but that, you know, HIPAA is basically equivalent to FIPS 200 or to the FISMA law itself and maybe that doesn't need to be changed, maybe all we need is a mechanism to update a guidance document more frequently.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

I like that. This is David. Guidance is what this sounds like to me.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, well that's, I mean we were sort of looking.

Paul Egerman – Businessman/Entrepreneur

That's probably right, yeah.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, I think that's right. I mean, we were not suggesting that the regulations necessarily needed to be changed although, you know, again, instead taking a look at bullet point number one, and we can certainly massage it to be more clear. We're sort of looking for a process and maybe what we need to do in this bullet is to emphasize the guidance piece of it more.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, the word policy is what scares me a little bit.

Deven McGraw – Center for Democracy & Technology – Director

Okay. All right. Well we don't need to scare people that makes...

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Well, it maybe that there's a policy need but the policy might be that the guidance be updated every two years.

Paul Egerman – Businessman/Entrepreneur

Yeah. So what we really should be saying is we should adopt a consistent more dynamic process for updating guidance regularly.

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

Yeah and I think that includes, I think a real problem in health care security is the fact that people don't do risk assessments. And maybe the reason why they don't is that they don't have good guidance on how to do it or whatever, but if we fix that, if organizations, regardless of their size, actually did risk assessment and implemented counter measures accordingly, you know, our security would be way better.

Paul Egerman – Businessman/Entrepreneur

Okay. So, on these two bullets on the screen, the comment I'm hearing from a couple of people is to be clear that the dynamic process we're talking about is really more dynamic guidance. I personally don't think we want to give a time period for the frequency of the guidance only because, you know, it's just really hard to predict, you know, what technological change or something that might occur in the frequency, but certainly we could say that the guidance is more frequent than sort of a regulatory process, but to clarify that we're talking about guidance in the first bullet.

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

And they'll need to create the guidance to begin with because there is nothing in health care that's equivalent to 800-53.

Deven McGraw – Center for Democracy & Technology – Director

So maybe it's really about issuing and regularly or consistently updating guidance.

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

Yeah.

Deven McGraw – Center for Democracy & Technology – Director

Without a timeframe.

Paul Egerman – Businessman/Entrepreneur

That's correct.

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

Yeah.

Paul Egerman – Businessman/Entrepreneur

Without a timeframe and I think we also want to capture the concept that the guidance must be for, besides being dynamic, it must be scalable is the right word, but, you know, to deal with the range of institutions that are involved, and it also has to be, do we need to include Leslie and Gayle's concept too? But there has to be a goal of at least a minimum security or baseline.

Deven McGraw – Center for Democracy & Technology – Director

Yes.

Gayle Harrell – Consumer Representative/Florida – Florida State Legislator

This is Gayle. I would say that's an absolute essential. There has to be a minimum, I really appreciate what Dixie is saying about the assessment, the security assessment needs to be part of the process as well. I don't know whether, I mean, we've addressed that other places, the risk assessment, but do we want to put something along that line in here as well?

Deven McGraw – Center for Democracy & Technology – Director

It is already required, Gayle.

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

Yeah and so is the baseline, HIPAA already has a baseline and already it requires risk assessment.

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

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

So the guidance should just tell them to do it periodically and when to do it, you know, personally I just don't know, how they should comply with HIPAA.

John Houston – University of Pittsburgh Medical Center – NCVHS

But I think the guidance needs to be actionable and what I mean by that is, and I'll give you a great example, when the Mass General settlement agreement, whatever you want to call it, came out one of the things that was said in the agreement was that Mass General needed to implement removal device encryption or USB device encryption. So, I use that frankly as, okay that's sort of a statement of position by OCR about what they expect all providers to do and we always had a policy that that's something people should do but we haven't enforced it on a mandatory basis. Well, we've been trying, since that time to come up with a viable solution to enforce and require USB thumb drive encryption in our environment and it's been a real challenge. So, I think whatever we do we'd better make sure that it's something that is actionable, that we can reasonably expect people to implement.

Neil Calman – The Institute for Family Health – President and Cofounder

So this is Neil Calman. I just wanted to throw in a couple of things and while we've been on the phone I've also been looking at that 800-53 document. So, a few things occur to me, the first is that there needs to be a major educational effort here if we really expect people to move in the right direction. I mean, very few providers have any clue about 90% of the things that I've scanned in the last half an hour, you know, and I think that that's something that people need, a lot of it has to do with physical environment about the work flows and the way information is handled and stuff, and people don't have a clue about this. Nobody is really trained in this area. And so I think the guidance really does have to be educational first off if we're going to get people to do this and you need that in order to do a risk assessment, you have to know what you're assessing and know something about it. So, I think the specificity is really important.

The second point I would make is that a lot of this stuff is so dependent upon setting. So, I really don't, I think in some of the areas it's, you know, minimum standards are going to be very difficult because, you know, just thinking about physical security of a space, you know, a private doctor's office and what does it mean when somebody can, you know, break in a window and steal their computer and what information is on it and, you know, what are we saying to people about that and in a large environment, you know, there's all kinds of passwords and electronic security devices that are being, you know, recommended. I mean, we really have to be, and I don't think it just has to say it needs to be context specific. I think we really need to say, you know, maybe even get down to the point of saying, you know, in a small doctor's office, these are things that can be done to maximize the security of the information whereas in a large institutional setting there are other standards that would apply, but I don't think just putting something out and saying well, you know, do a risk assessment really creates the model.

And then the last point is that, you know, remember as information is passed from place to place it's only as secure as the least secure place it sits.

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

Neil Calman – The Institute for Family Health – President and Cofounder

And so, you know, a hospital can have all the major security devices and do a risk assessment and put in all, you know, meet everyone of these kinds of standards, and then the doctor's office accesses the patient's information and puts it on their PC, you know, in an unlocked, unsecure environment and leaves it open on the desk when another patient is there. I mean, you know, I think that's part of why we're talking about minimum standards, but I think what we're trying to do is very difficult and I think should start with a major educational effort and some documents that we would call out to be produced that really give people guidance about how to do this. This is something everybody wants to do but nobody, you know, at least that aren't expert in this already knows even how to begin this process.

Paul Egerman – Businessman/Entrepreneur

So, very helpful comment. So the major things that I'm hearing from what you are saying Neil is, you know, we have to go beyond just saying scalable. You want to give some specific examples in common settings so that it's clear and we should be recommending some sort of an educational component too, to help people understand what they are supposed to be doing.

Neil Calman – The Institute for Family Health – President and Cofounder

Well and give them very specific examples of meeting this that are, you know, consistent with their capabilities in the environments that they set.

Paul Egerman – Businessman/Entrepreneur

It's dynamic through guidance, it's scalable it's got specific examples.

Neil Calman – The Institute for Family Health – President and Cofounder

I mean, I've learned so much just by reading through this.

Paul Egerman – Businessman/Entrepreneur

And some level of educational component.

Neil Calman – The Institute for Family Health – President and Cofounder

Yeah.

Gayle Harrell – Consumer Representative/Florida – Florida State Legislator

Paul add the REC to the component because I think the place that this needs to, at least part, is to educate through the RECs. I think that we could call them out as well.

Paul Egerman – Businessman/Entrepreneur

That's true. Well, I think we could add RECs as an example. There might be other ways you do education too though.

Gayle Harrell – Consumer Representative/Florida – Florida State Legislator

That should be perhaps one of the charges to them, very specifically, hands on kind of instruction to the, especially the small practices.

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

I think it is in HITECH calls out the RECs do security.

Paul Egerman – Businessman/Entrepreneur

Yeah I think so.

Deven McGraw – Center for Democracy & Technology – Director

Well we can check on that but I think it's worth mentioning as well.

Paul Egerman – Businessman/Entrepreneur

So, I think though, I'm hearing, I mean, Deven and I have to do some wordsmithing, but I'm hearing a consensus about guidance, dynamic, specific examples, scalable, education mentioning RECs, but also as I said specific examples. I want to turn a minute to the second bullet on this screen, which is simply a recommendation to HHS, evaluate the gap analysis with a goal to closing the gaps, closing the gaps might be the same thing as resolving the gaps. In other words, you could lower the gap and you could decide you're not going to do anything with that gap within a reasonable period of time, and time could be like, I don't know, it's probably going to take several years to do would be my guess. Is this something we should be making a recommendation on? In other words is the first recommendation enough or do we also want to say that HHS should be doing this gap analysis comparing these other frameworks with what is in the security rule.

Deven McGraw – Center for Democracy & Technology – Director

And we could, as I think about this bullet, Paul, this is Deven, relate this to the guidance.

Paul Egerman – Businessman/Entrepreneur

That's right. In other words, the result of resolving or closing the gap might be guidance to do something. It might be guidance to do something for a large organization, you know, it's really hard to know, but that would be how you could resolve a gap or close a gap, it could be a decision you don't need to do anything at all for whatever reason it's not anything to do but still you go through some process of evaluating where the gaps exist.

Gayle Harrell – Consumer Representative/Florida – Florida State Legislator

This is Gayle. I think that's absolutely essential.

John Houston – University of Pittsburgh Medical Center – NCVHS

This is John Houston. Should this though potentially be something that we look to HITRUST for instead of HHS if we think it's going to take, you know, two years to be able to do updates? I think there are other organizations that are more focused on this or potentially are going to be more nimble at providing guidance and gap analysis and recommendations.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, but at the same time, John, I don't disagree with the nimbleness point, but at the same time, you know, HIPAA and whatever other sets of rules that ONC might promulgate related to the HITECH financial incentive programs, like those are the, HITRUST is voluntary, the meat of what people are required to comply with vests in, you know, the policy levers that HHS has, and if they want to rely on some voluntarily developed guidance to issue their own guidance I think that that's perfectly fine, but at the end of the day I think people need to understand what is expected of them in terms of compliance with the law or other specific requirements and I don't think you can default that or punch that totally to a private entity.

John Houston – University of Pittsburgh Medical Center – NCVHS

No your right.

Paul Egerman – Businessman/Entrepreneur

Well maybe there's a way to reconcile this with what you just said, is we brought in this gap analysis and view that as sort of like also a continuing process, because in theory all these other frameworks will be changing over time and HHS should be evaluating, doing a gap analysis between the HIPAA security rule and other security, you know, other government security frameworks and other commonly used frameworks with the idea of using that information to determine if there are reasons to change guidance.

John Houston – University of Pittsburgh Medical Center – NCVHS

Right.

Paul Egerman – Businessman/Entrepreneur

To me it's just like I hear HITRUST, I shrug my shoulders, I say well is there something to be learned there, if there is let's learn it.

John Houston – University of Pittsburgh Medical Center – NCVHS

Well the other piece of this too is that, you know, they're going to start doing audits pretty soon. I guess they've already begun to do audits and...

Paul Egerman – Businessman/Entrepreneur

Good for them, that's good.

John Houston – University of Pittsburgh Medical Center – NCVHS

But, no, no I'm talking about the ONC, who have they hired to do audits, I know it's a big press release; they're going to do 120 or however many over the next year.

Deven McGraw – Center for Democracy & Technology – Director

That's OCR.

John Houston – University of Pittsburgh Medical Center – NCVHS

Oh, I'm sorry, OCR.

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

John Houston – University of Pittsburgh Medical Center – NCVHS

And the question is that any time an auditor comes in to audit anything there's an audit plan underlying an audit, I mean that's basic principles of auditing. The question is, is what are the audit plans that they're going to use to audit people and does that also provide some guidance as to what the expectations OCR has with respect to covered entities and their compliance with HIPAA.

Paul Egerman – Businessman/Entrepreneur

That's a good question, but the way I interpret that question is people would like to get this guidance, right.

John Houston – University of Pittsburgh Medical Center – NCVHS

I'd like to get the audit plan.

Paul Egerman – Businessman/Entrepreneur

Well if you're operating according to guidance you have an answer for the audit. I did what it says here I that I'm supposed to do.

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

I think that's an 800-53a equivalent, but, you know, I think it's downstream, but I have a concern though. This is Dixie. I know that a lot of health care organizations across our whole industry are very sensitive to having, you know, forcing private industry to comply with federal rules and FISMA clearly is a federal rule. Has this kind of exercise been done against ISO 27001?

Paul Egerman – Businessman/Entrepreneur

Well that's a question I don't know the answer to.

Deborah Lafky – Office of the Chief Privacy Officer

This is Deborah; perhaps I can help with that. Dixie one of the things that we did was also to crosswalk FISMA to ISO 27001, Kevin did include that as part of his analysis and we have not presented the whole analysis here, but the objective of the exercise was to sort of demonstrate the gaps between the security rule and security frameworks in general with the assumption, which is borne out by the evidence that these frameworks are very similar in their structure and in their requirements and if you look at the families that are in ISO versus the families that are in FISMA, they are almost identical and if you go out to say CoBIT you'll find, again very, very high degree of similarity in the way they're structured.

Paul Egerman – Businessman/Entrepreneur

I have to interrupt just a little bit, because as Deven said, we're on an unusual timeframe, we're supposed to end at 1230 and we have five minutes left and we need to leave a few minutes for public comment. So what I'd like to understand is where we are in this discussion. Are we at a point where people feel okay that we can draft some, Deven and I should draft some wording on these recommendations and sort of wordsmith it through email, or do you feel we need to have more discussion on these topics?

Deven McGraw – Center for Democracy & Technology – Director

I would like, personally, Paul this is Deven, I would like to try to, I feel like we're close, I think we have to be careful to talk about HHS using, you know, resources to develop its guidance that aren't just limited to this particular gap analysis, but certainly this has been done and they should look at it when they do guidance issues, but I feel like we're close and I feel like we could try to wordsmith it. I mean we do have another call on the calendar should we need to, but it feels like its close.

Paul Egerman – Businessman/Entrepreneur

Yeah, but I want to find out what other people think.

Deven McGraw – Center for Democracy & Technology – Director

No, I know.

Judy Faulkner – EPIC Systems Corporation

This is Judy and I was, the one thing I didn't hear, but I did join the meeting late and I apologize, is there any way, and tell me if it has nothing to do with it and we can't do this, that we can also make sure that as we add this we don't increase paperwork. I've just spoken to one specialist who was just at a wedding and he just came up and said he is quitting his job because he can't deal with the paperwork and I was listening later to three primary care physicians talk about how they can't, they were from different states, they can't get dental care for the indigent folks, patients because the dentists refuse to do it because of the paperwork. Going back to some of the discussion we have about being careful about the small practitioners I wonder if we could also be careful about the paperwork for them.

Paul Egerman – Businessman/Entrepreneur

Okay. So the question still is, are we close enough to...

Judy Faulkner – EPIC Systems Corporation

Yeah, well I wanted to throw that in.

Paul Egerman – Businessman/Entrepreneur

That was a good comment.

Neil Calman – The Institute for Family Health – President and Cofounder

Paul?

Paul Egerman – Businessman/Entrepreneur

Yeah go ahead, Neil.

Neil Calman – The Institute for Family Health – President and Cofounder

Yeah, just, you know, in the second bullet I think we should eliminate the part that says closing the gaps.

Deven McGraw – Center for Democracy & Technology – Director

Yes.

Paul Egerman – Businessman/Entrepreneur

Yes, I agree.

Neil Calman – The Institute for Family Health – President and Cofounder

Because we don't really know if we want to close the gaps until we look at what the gaps are.

Deven McGraw – Center for Democracy & Technology – Director

Yep.

Paul Egerman – Businessman/Entrepreneur

Yes, it's really to look at those...

Neil Calman – The Institute for Family Health – President and Cofounder

I think if we're evaluating it, but at least from the stuff that I've been looking at, you know, a lot of these gaps we don't want to close, you know, some of them about physical plant and things, they're just not realistic to be closed. So, I think we should just stop and say we should evaluate the gaps for sure, and I would just end it right there.

Paul Egerman – Businessman/Entrepreneur

Yeah. I agree with that. The purpose of evaluating the gaps is to see where gaps might exist; it does not necessarily mean we have to respond. Here's what I want to suggest, because we do have to end close to on time and its 12:30. So, here's what I suggest, is Deven and I will circulate an email where we'll try our best to capture this discussion and simply ask you if you're happy with it great, if you want to continue and have another meeting we could do that also. Does that work for everybody?

John Houston – University of Pittsburgh Medical Center – NCVHS

Yes.

Paul Egerman – Businessman/Entrepreneur

Okay. So unless you have something you would like to add, Deven, I think we need to open the line for public comment. Do you have any comments Deven?

Deven McGraw – Center for Democracy & Technology – Director

No, let's go to public comment.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Operator would you please check and see if there's anyone who would like to make a public comment?

Caitlin Collins – Altarum Institute

Yes. If you are on the phone and would like to make a public comment please press *1 at this time. If you are listening via your computer you may dial 1-877-705-2976 and press *1 to be placed in the comment queue.

Verne Rinker – Office for Civil Rights

While we're waiting, this is Verne, I just wanted to throw one thing out there, which is the HITECH 13401 requires us to do security rule guidance on an annual basis and last July we published guidance on the risk analysis. So, I haven't heard that come up as a model or a currently going on activity. So, I would at least like folks to be aware that that's there, that it's on our website, because it sounds like that's right down the alley of the recommendations.

Paul Egerman – Businessman/Entrepreneur

That's very helpful.

Deven McGraw – Center for Democracy & Technology – Director

What was the statutory reference, Verne?

Verne Rinker – Office for Civil Rights

13401, I believe its c.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

Paul Egerman – Businessman/Entrepreneur

So we should look at that.

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

Mary Jo Deering, Ph.D – Senior Policy Advisor – Office of the National Coordinator for Health Information Technology

Operator are there any public comments?

Caitlin Collins – Altarum Institute

We do not have any comments at this time.

Paul Egerman – Businessman/Entrepreneur

Okay, well thank you very much. Let me thank all the members of the task force, this is extremely important discussion and I appreciate the focus and spirited comments. Of course I want to thank Verne and Deborah Lafky and who else should I be thanking, Deven?

Deven McGraw – Center for Democracy & Technology – Director

Kevin Stine.

Paul Egerman – Businessman/Entrepreneur

And Kevin, absolutely for your presentation.

Kevin Stine – National Institute of Standards and Technology

Thank you.

Paul Egerman – Businessman/Entrepreneur

Thank you very much.

M

Bye-bye.

Paul Egerman – Businessman/Entrepreneur

Bye-bye.