



HIT Policy Committee Privacy & Security Workgroup Final Transcript February 9, 2015

Presentation

Operator

All lines bridged with the public.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Thank you. Good afternoon everyone this is Michelle Consolazio with the Office of the National Coordinator. This is a meeting of the Health IT Policy Committee's Privacy and Security Workgroup. This is a public call and there will be time for public comment at the end of the call. As a reminder, please state your name before speaking as this meeting is being transcribed and recorded. I'll now take roll. Deven McGraw?

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Deven. Stanley Crosley? Adrienne Ficchi? Bakul Patel? Cora Tung Han?

Cora Tung Han, JD – Division of Privacy and Identity Protection, Bureau of Consumer Protection – Federal Trade Commission

Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Cora.

Cora Tung Han, JD – Division of Privacy and Identity Protection, Bureau of Consumer Protection – Federal Trade Commission

Hi.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

David Kotz?

David F. Kotz, PhD – Associate Dean of the Faculty for the Sciences – Dartmouth College

Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, David. David McCallie? Deb Bass? Donna Cryer? Gayle Harrell? Gil Kuperman? Gwynne Jenkins?

Gwynne L. Jenkins, PhD, MPH – Senior Policy Advisor to the Director, OCRBP – National Institutes of Health

Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Gwynne. John Wilbanks?

John Wilbanks – Chief Commons Officer – Sage Bionetworks

Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, John. Kitt Winter?

Kitt Winter, MBA – Director, Health IT Program Office – Social Security Administration

Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Kitt. Kristen Anderson?

Kristen Anderson, JD, MPP – Staff Attorney, Division of Privacy & Identity Protection – Federal Trade Commission

Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Kristen. Linda Kloss? Linda Sanches?

Linda Sanches, MPH – Senior Advisor for Health Information Privacy – Office of Civil Rights

Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Linda. Manuj Lal? Mark Sugrue? Micky Tripathi? Sephania Griffin? Taha Kass-Hout? And from ONC do we...

Taha A. Kass-Hout, MD, MS – Director, FDA Office of Informatics & Technology Innovation – Food & Drug Administration

Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Oh, sorry about that. From ONC do we have Helen Canton-Peters?

Helen Canton-Peters, MSN, RN – Office of Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

I'm here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Helen. And Kathryn Marchesini?

Kathryn Marchesini, JD – Acting Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Kathryn and with that I will turn it back to you Deven.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

All right, great, thank you very much Michelle. Just want to thank everyone who was able to join us on the call today as well as members of the public who are listening in we're continuing our discussions about health big data and we have a treat today we're going to hear from three experts in the area of health data security to help us think through the security issues.

We had presentations from a number of folks back in December on a range of more privacy related issues but we realized fairly quickly that we did not get sufficient input on the security aspects of health big data and we're fortunate to be able to have three people with us today who will help us to begin to think through the issues, identify those issues and think through what recommendations we might come up with to help resolve them so that we can maximize the opportunities from health big data that we know are out there.

Just to give you a sense of sort of where we are in terms of our work overall as a working group. As you'll see we've been, for four of our previous meetings, we have taken on this topic of health big data and again we're going to continue on that theme today beginning with security issues first but then seeing if we can make a bit more progress on some of the issues around consent that we began talking about on our previous call.

And then as you'll see from the slide which is, if we have people who are sort of following along on paper I'm on slide three on the work plan, we're going to have to make a bit of a shift in our focus in order to review the draft interoperability roadmap which ONC has released for public comment and that will be the subject of presentations that will take place at the Joint Health IT Policy Committee and Health IT Security Committee meeting which takes place tomorrow if you want to listen in on that.

And we will be tasked with reviewing and commenting on specific aspects of that plan and given that the comment period has a deadline we do need to turn to that expeditiously and we will return to our health big data work when we have finished our work on the interoperability roadmap.

We are slated to at least begin to give a progress report to the Health IT Policy Committee at the March meeting but in no way will we be ready to present final recommendations. We still have, I think, a considerable amount of work to do on the health big data issues although we're certainly making progress. So, just to give you a sense of where we are.

I also want to, before we turn to our panelists on security, remind the Workgroup about what is in scope and not in scope for our health big data conversation because health big data is one of those topics with lots and lots of pieces to it. Our particular purview is to look at the privacy and security issues that arise both with respect to the concerns but also potential barriers that often get enacted with the good intention of protecting privacy and security of health data but may have posed some barriers to progress or innovation. And then potential harmful uses of health data or data that has implications for health that are related to privacy.

What we're not going to consider, because it's really out of the scope of our working group are issues involving data quality and data standards and the non-representativeness of data that often time's data is not representative of the population and yet we're relying on it to tell us all sorts of things about the population. So, we're not trying to resolve that issue from the stand-point of how do you increase the representativeness of data but certainly we can and should consider it from the context of harmful uses.

And so with that, I think we're going to move to hearing from our presenters on the issue of data security. I'm going to call on you in the order of the agenda and briefly introduce each of you before you speak. We'll have Andrei go first, Denise go second and Ryan go third.

Customarily in these presentations you have five minutes to give us an overview of what you'd like us to consider and then after each of you have had your five minutes to present there is a period of questions from the working group members. Five minutes goes way too fast and my sincere apologies for that because there are only three of you I'll try to give you all each a bit of leeway but inevitably what happens is that you probably will run out of time unless you've timed yourself but we'll make sure that you have an opportunity during the Q&A to iterate any points that you either had to go over too fast in your presentation or that you missed being able to highlight at all because you just didn't have enough time.

And customarily in our...when we've asked people to present to us before the combination of, you know, a brief five minute or so presentation at the front and the Q&A usually results in sort of a full airing of what you wanted to present and we hope that will be the case today. Does anybody have any questions either from working group members or from panelists before we get started?

Okay, was there anybody who missed roll call who is on now and wants to identify themselves?

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Hi, Deven, it's Lucia, I'm here.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Okay, great, thanks.

Manuj Lal, JD – General Counsel, Corporate Secretary & Chief Privacy/Information Security Officer - PatientPoint Enterprise

Hi...

Gilad J. Kuperman, MD, PhD, FACMI – Director Interoperability Informatics – New York Presbyterian Hospital

Gil Kuperman here.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Oh, great, hi, Gil.

Gilad J. Kuperman, MD, PhD, FACMI – Director Interoperability Informatics – New York Presbyterian Hospital

Hello.

Manuj Lal, JD – General Counsel, Corporate Secretary & Chief Privacy/Information Security Officer - PatientPoint Enterprise

And you've got Manuj as well.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Hey, Manuj, great.

Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP

Stan is here too, Deven.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Oh, awesome. I figured you all were there.

Stephania Griffin, JD, RHIA, CIPP, CIPP/G – Director, Information Access & Privacy Office – Veterans Health Administration

And this is Stephania Griffin.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Hi, Stephania, terrific. Anybody else? Okay, with that we will turn to Andrei Stoica who is Vice President of Global Systems Development and Security at IMS Health. Dr. Stoica, are you ready?

Andrei Stoica, MS, PhD – Vice President Global Systems Development & Security – IMS Health

Yes, thank you, Deven.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Okay, we're ready when you are.

Andrei Stoica, MS, PhD – Vice President Global Systems Development & Security – IMS Health

Today I want to talk a little bit about complexity in information security. It's often times that we spend, as a practitioner, we spend a lot of time dealing with incidents. There is a vulnerability in a browser if something happened, there is a leak of data and we spend a lot of time doing this and often times we don't see the forest from the trees. So, today I want to just take a step back and say...and look at how do we actually approach security from a holistic perspective?

The reality is there is a lot of complexity in software development and it has been proven mathematically, I'm not going to get into that theory, that there is no...you cannot build a single program to test a piece of software, you can to a certain extent, for certain exceptions but it has been proven that you cannot do this Alan Turing proved that 60-70 years ago. What that means is that we're always going to have bugs and security vulnerability that's always going to happen. So, the question is how do we deal with this?

We have complexity in the software embedded in almost every piece of hardware that we use in healthcare from simple temperature devices to complex MRI machines that use software. We have software that runs the network; we have software in large applications from EMR to claim processing to financial systems. When you put all of this together you end up with a very complex system that will have flaws and these flaws get exploited and that's how we have vulnerabilities. So, how do we deal with this?

One of the really hard lessons learned from the past 20-25 years in security is that you have to have a holistic approach. You have to look at your operations end-to-end and you have to apply a risk-based framework. Early attempts to focus on narrow standards failed because security in contextual one method that works today very well in some context is going to be very vulnerable in another context tomorrow.

There is no such thing as zero risk. The only way to...the anecdote is the only way to get 100% security from a computer system is to turn it off. And if you don't approach security from a holistic perspective you run the risk of overlooking some areas and again the analogy here that is used in security is, there is no point in having a steel door at the entrance with a sophisticated lock if you actually have an open window.

And the last point I want to make here is that the threat landscape varies over time. The security objective should be based on outcomes not the means because the means change constantly, the hardware, the software, the attack mitigation everything changes sometimes daily. And the only pragmatic way to secure data in healthcare and in any other domain is to consistently follow an industry developed risk-based framework.

We have in place legislation such as HIPAA that defines the high-level objectives and what we need on top of that is an industry developed risk-based framework that will define very specific, contextual and evolving controls that apply to reduce risk down to an acceptable level.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Okay, terrific.

Andrei Stoica, MS, PhD – Vice President Global Systems Development & Security – IMS Health

Did I make my five minutes?

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Yeah, you were like 3.5, you did very well.

Andrei Stoica, MS, PhD – Vice President Global Systems Development & Security – IMS Health

Oh, I did, then I am prepared for questions.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Yeah, you absolutely do, so we'll have the other two presenters go and then all three of you will be able to answer questions, so thank you very much for that presentation that was very helpful. Okay, so next we have Denise Anthony who is the Vice Provost for Academic Initiatives and a Professor of Sociology at Dartmouth College. And Denise, I think you...yeah, there they are. So, all you need to do for your slides is just say "next slide" and the folks at Altarum who help us run our meetings will move them for you.

Denise Anthony – MA, PhD - Vice Provost for Academic Initiatives & Professor of Sociology - Dartmouth College

Okay, I'm going to probably go fast because I probably have too many slides.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Which is okay, I can give a little leeway, you can borrow some time from Andrei how about that?

Denise Anthony – MA, PhD - Vice Provost for Academic Initiatives & Professor of Sociology - Dartmouth College

Okay, thanks, but certainly jump in whenever you need me to stop...

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Okay.

Denise Anthony – MA, PhD - Vice Provost for Academic Initiatives & Professor of Sociology - Dartmouth College

If I'm still going.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Okay.

Denise Anthony – MA, PhD - Vice Provost for Academic Initiatives & Professor of Sociology - Dartmouth College

So, thanks a lot, I just want to start with just the brief acknowledgements which are on slide two which are that some of the work I'm going to talk about is based on an NSF Grant and then also on the SHARPS Grant from ONC, and a variety of collaborators including David Kotz, who is on the phone, but also Ajit Appari, Celeste A. Campos-Castillo, Carl Gunter, Eric Johnson, Sean Smith and Tim Stablein who are all co-authors on various work.

And what I want to do is talk a little bit about...a lot of my work has been on privacy issues but I'll try to then connect that to at least the transparency and consent issues that you're going to get to and then just talk a little bit about HIPAA compliance in hospitals. Next slide.

So, we know that from many studies that patients value EHRs for both themselves and their providers and we also know that there is a strong connection between when a provider uses EHRs and the quality of care rating that patients give them. However, when we really control for all of these different factors related we still do find a connection between patient's willingness to disclose information and patients being more likely to withhold information when a provider uses an EHR and withholding information because of concerns about privacy.

And then further there are particular groups who are more likely to withhold information and these groups are at least those who are at risk of health related stigma or social stigma and in general we find that those groups have less trust in the confidentiality of their physicians in general and they're more likely to express concerns about disclosure and especially with EHRs though these groups generally also note that when they have a trusting relationship with their provider they are willing to disclose even with EHRs. So, next slide.

The implications of this are that despite the increase and concern we can see that doctors and health providers can really facilitate communication and trust by patients if they acknowledge and discuss the privacy concerns with their patients.

And so just a recommendation from this research is that to really promote transparency about information flows of this kind of data whether it's big data or data in your electronic medical record or coming from different devices is that the notice of privacy practices is sort of a minimum at best and that providers should be encouraged to discuss these things with their patients because it means a lot coming from a physician. So, I'll move on quickly to the next issue. So, next slide.

We wanted to ask consumers a little bit more about their expectations about what kind of disclosure is already happening or their ability to find out about disclosures of their health information. In the spring of 2014 we did a national random probability sample of the US population of adults, a resulting survey of 784, those are just the demographics. I'll go to the next slide and actually this slide just shows that we find what other studies have found, which is people value EHRs they value electronic exchange of information.

And next slide is starting to get at their expectations about disclosures that are happening with their PHI. So, when we ask them on a scale of 1-5 strongly agree to strongly disagree if it is important for them to find out who has looked at their medical records we find 66% say they agree or strongly agree. Even more telling I think is the next question in which we asked whether they strongly agree or strongly disagree with this statement "I should be able to find out who my doctor discloses my medical information to" and there we found 91% agree or strongly agree that they should be able to find out who their information is disclosed to.

And so...and just to take that a little bit further in the next slide, we asked them how confident they were, this is a slightly different way of getting at the information rather than just saying how strongly do they agree but do they already feel confident about the control over their information, their health information and what protections might exist. And so we asked them on a 3-point scale a very confident, somewhat confident and not confident and so the first statement was "I had some say in who is allowed to collect, use and share my medical information." Here we find, as in all of these, about 1/3 say they're very confident, about half say they're somewhat confident and here under 20% say they're not confident about this. It's not clear whether you see this as good news or not good news, but they are demonstrating that about 1/3 of the population is really already expecting that they have this say.

The second question was “I have some say in whether my information is shared with anyone other than my regular provider or my doctor.” Again, we see similar percentages across the three.

And the third question is more about the generic protections in place not just from their doctor but in the healthcare system and this question is “safeguards including the use of technology are in place to protect my medical records from being seen by people who aren’t authorized to see them.” And again, we see about 1/3 of the population being very confident and just a little aside here in how this relates back to the role of the providers themselves both the clinician and the provider organization is that those who have high levels of trust in their positions already are more likely to say they have this confidence because they’re having conversations with their providers.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Yeah, so, Denise.

Denise Anthony – MA, PhD - Vice Provost for Academic Initiatives & Professor of Sociology - Dartmouth College

Yes?

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

I know we’re probably not even...I don’t know where we are in your presentation but you’ve had about 6.5 to 7 minutes.

Denise Anthony – MA, PhD - Vice Provost for Academic Initiatives & Professor of Sociology - Dartmouth College

Okay.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

But having said that you have slides so is it possible for you to sort of let us know what else you have so we can prompt you with some questions so we can get it out during the Q&A?

Denise Anthony – MA, PhD - Vice Provost for Academic Initiatives & Professor of Sociology - Dartmouth College

The, you know, slides 10 and 11 are about HIPAA compliance in hospitals.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Okay.

Ryan Andersen – Information Technology Consultant Network Administrator - Milliman

This is Ryan; mine won’t take 5 minutes she can have a couple more minutes and then we’ll still be okay.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

You and Andrei are very generous, okay, go ahead Denise.

Denise Anthony – MA, PhD - Vice Provost for Academic Initiatives & Professor of Sociology - Dartmouth College

Okay, well thanks, so if you want I can just go directly to slide 10. This is research on US hospitals with 50 or more beds and we were looking at the earliest days of HIPAA compliance so in 2003 when the privacy rule became mandated and so the take home point of this research is that compliance...HIPAA compliance varies a lot across hospitals because hospitals have different levels of resources to begin with, they respond to compliance in different ways with different practices and they seek to comply for different reasons and so it just means that I think a take home point is that any kind of regulatory incentive or effort has to be prepared for this level of variation across US hospitals and US providers in general and I'll just stop there.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Okay, great, thank you, very much Denise and don't go anywhere because we'll have a Q&A period. Okay and so our third presenter is Ryan Andersen who manages operations in the Applications Services Provider area of MedInsight for Milliman and we're happy to have you Ryan. Are you ready?

Ryan Andersen – Information Technology Consultant Network Administrator - Milliman

Sure. So, just really quickly as MedInsight for those of you that don't know we are a data aggregator and so when it comes to big data we are, you know, on the leading edge of aggregating data from multiple different suppliers of it and once it comes to us it becomes bigger and bigger data.

And so when we consider the, you know, when we're considering security and privacy we're probably doing it at a little bit different level in that we're actually not thinking of necessarily electronic health records we're thinking about entire sets of data and the entire set of data is as though it were a patient and it's considered very private.

That being said the other...while we're trying to keep it secure the other thing that we're trying to do is we're trying to share it and so as a data sharer we aggregate this data and people want us to aggregate this data so that we can share it with other people either themselves or potentially subscribers to what it is that they're trying to accomplish. The benefits of that are, you know, the most striking one is obvious and that is through the sharing of this big data through the using of this information we can potentially make improvements not only to healthcare but to the healthcare system and so we're at a bit of a disadvantage when we talk about that because as we've seen recently, you know, in the news, even if you're trying not to share data sometimes that data gets shared, you know, because it gets attacked and people find a way in and so we are...we find ourselves in kind of an unenviable position of being...wanting to share that data but not wanting to share it with the wrong people and so we kind of have to have the door halfway open which makes our security concerns even more so difficult to implement.

One of the things that is important when we're talking about protecting data is who are we protecting it from. In our industry or in our business we're just trying to protect it from people that don't, you know, that aren't supposed to see it or that may do, you know, may be nefarious things with it. But that range of people is huge, it could be anybody from, you know, a foreign government to, you know, somebody in their mother's basement or something like that. And so the variety of different intrusion is certainly wide and seemingly never ending.

And so what we've done is we've determined that rather than be necessarily externally focused all of the time on protecting the castle gate, if you will, one of the things that we've started to do is look internally at the data itself and that is in so much as in the work that we do we're trying to ask ourselves what is it that we're actually...what is it that we need to house, host, pardon me, or what is it that we need to protect.

And so rather than in today's world of technology it's really easy for us to get a lot of information and I think that one of the things that we're focusing on and it might be a good idea for the industry to focus on is rather than protect, you know, protect something which is almost unprotectable because people are going to find a way in because they're going up against other people, they're going up against software that was created by human beings.

I think Dr. Stoica said it at the very beginning like we just...it's almost like it's not possible to protect it. So, instead of that we should look internally to say, all right well what is it that they're going to see if and when they get in and make better efforts to limit that dataset to what's really necessary.

For example, in the work that we do social security number, we will get that information from a lot of people and rather than get that we should ask them to send us something that's hashed and protected on the way in because there really is no point in having some of this information because all it is...it makes a valuable or paints a target on us and says that is very valuable information whereas it's not valuable in the work that we're doing and so that is one of the...well that's actually the focus of what we're working on recently is focusing internally rather than externally as to what it is that we can do to help protect people's information when that information really isn't necessary and that...

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

All right, terrific. Thanks to all three of you and very much appreciate again your taking the time to be with us this morning. I want to open it up to our Workgroup members to ask you questions. Does anybody have any already queued up? I don't...we'll just use the verbal...I'll just call on people verbally.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Deven, this is Lucia, I have one for Denise.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Sure, go right ahead.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Denise did your survey instrument have any contemporary findings regarding whether people thought the information that their physicians had electronically whether they thought it was safe as opposed to their preferences about what they were going to be told about its use which is an important but different question than security?

Denise Anthony – MA, PhD - Vice Provost for Academic Initiatives & Professor of Sociology - Dartmouth College

Yes, so we...yes, we have a question and I'm going to actually...

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

If you want to tell the Altarum people which slide I'm sure they could pull it up.

Denise Anthony – MA, PhD - Vice Provost for Academic Initiatives & Professor of Sociology - Dartmouth College

It's not on the slide but we asked a question that said, I'm just going to read it off the...that said "in general I think that the information I give doctors is safely guarded" and it was an agree or disagree question.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

And did it distinguish between information that was captured in an electronic system versus a file folder system, you know, paper?

Denise Anthony – MA, PhD - Vice Provost for Academic Initiatives & Professor of Sociology - Dartmouth College

No, this one just says, do you, you know, agree that the information...how strongly do you agree or disagree that it is safely guarded. So, it's not distinguishing on this one between electronic records. This survey we haven't...I'm just presenting some preliminary results...

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Right.

Denise Anthony – MA, PhD - Vice Provost for Academic Initiatives & Professor of Sociology - Dartmouth College

But we do have a lot of questions but on this one we find that most people or ¾ of people, 77% or so agree or strongly agree that the data they give...the information they give physicians is safely guarded.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Okay.

Denise Anthony – MA, PhD - Vice Provost for Academic Initiatives & Professor of Sociology - Dartmouth College

So, it does...

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Timely this week.

Denise Anthony – MA, PhD - Vice Provost for Academic Initiatives & Professor of Sociology - Dartmouth College

Yeah, yeah 25% or so either are neutral or disagree with that statement.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Okay.

Manuj Lal, JD – General Counsel, Corporate Secretary & Chief Privacy/Information Security Officer – PatientPoint Enterprise

Deven, this is Manuj, I have a question.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Yeah, go ahead Manuj.

Manuj Lal, JD – General Counsel, Corporate Secretary & Chief Privacy/Information Security Officer – PatientPoint Enterprise

In your study or maybe even outside do we have any good research that helps us understand the use of mechanisms like in accounting of disclosures or the different, you know, mechanisms that are available to patients and whether they actually use them. Have you addressed that in your study?

Denise Anthony – MA, PhD - Vice Provost for Academic Initiatives & Professor of Sociology - Dartmouth College

So, we have a study right now where we're trying to get some...we have a different survey right now that just came in and trying to understand how often from the provider's perspective patients are asking for information like accounting of disclosures and it's...I would say it's still relatively low from the evidence that we are seeing there and the only caution I would throw out on that is in beginning this research we looked a lot at the early days of the Fair Credit Reporting Act and in the late 60s in the hearings, and maybe you guys have already looked at this and if so you can stop me, but there were hearings about, you know, making basically the FIPS, the early FIPS privacy allowances that said consumers should be allowed to be told who their credit record has been disclosed to and in those hearings leading up to that the data aggregators and the credit agencies basically said look there aren't any people asking for that information and so...and there was various...the evidence that they had showed very few people coming forward to ask for that information. And so...and yet they still put it in place and we still find that it's very useful for people to have.

So, looking for evidence of patients asking for accounting of disclosures I think is a bit problematic. This is partly why we asked the question that said "how important is it, do you think that you should find out who your information has been disclosed to" and 91% say they think that's important. So, I think...

Manuj Lal, JD – General Counsel, Corporate Secretary & Chief Privacy/Information Security Officer – PatientPoint Enterprise

Right. Yeah, so if there is a gap, right, I guess I'm trying to understand if there is a gap for people wanting to see it versus actually executing on their desire. I'm wondering if there is any study that has been done or maybe your survey will provide some insight into that.

Denise Anthony – MA, PhD - Vice Provost for Academic Initiatives & Professor of Sociology - Dartmouth College

Right I think that's exactly right most people trust their physicians and their providers around the information practices so I don't think a lot of people will be asking for that information and yet what we show is that most people expect that they could and so that's the...that's sort of the conundrum a little bit.

Manuj Lal, JD – General Counsel, Corporate Secretary & Chief Privacy/Information Security Officer – PatientPoint Enterprise

Got it, thank you.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Other questions?

Gilad J. Kuperman, MD, PhD, FACMI – Director Interoperability Informatics – New York Presbyterian Hospital

Hi, Gil Kuperman here, thanks to all the presenters. I have a question for Andrei Stoica. So, Andrei you used a phrase, you know, an industry developed risk-based framework, you know, kind of noting that, you know, HIPAA is in place but kind of below that, you know, there aren't really kind of guidelines and, you know, people try their best and, you know, then things happen and, you know, you kind of penalize them after the fact for not having appropriate procedures in place but that may not be great.

So, if I understood correctly you were proposing, you know, an industry developed risk-based framework and I guess my question is, you know, are there any candidates for such a framework in place, you know, are we close or would that be kind of a large task if we, you know, set about trying to create that kind of a framework. And I'd be eager to get your thoughts on that and then I'll have a quick follow up question.

Andrei Stoica, MS, PhD – Vice President Global Systems Development & Security – IMS Health

The good news is we actually have something that's almost developed and encompasses a lot of areas. So, we've been using HITRUST, it's been developed using a lot of the standards looking at previous industry developed standards from different industries, PCA, COBIT looking at ISO standards. There have been a lot of work in putting all of that together and really adapting it to healthcare. It is US centric but it has been looking at other standards globally so it's something that can actually be used even for global companies. We've been using this at IMS and really when we looked at all the standards we found that there were guidelines very specific for each area in development.

As I mentioned during my speech is security is really something that needs to be looked at holistically and something like physical security is not something that people usually consider, but there is no point in using, for example, very sophisticated firewalls and having your office wide open so somebody can come in and grab a laptop that's the balance that you need to look at and that's why you need a framework and HITRUST is something that is looking at all these aspects of security not just the typical that you get in the news, you know, firewalls, encryption at REST.

And another example that has been in the news a lot encryption at REST. That's useful in certain circumstances, for example if you have a mobile device, if you have a laptop that travels outside of your office yes it's very important that you have encryption at REST.

Do you need encryption at REST for let's say your mainframe that sits in a data center that's guarded with people with machine guns, I've never heard in my 20 something years in computer science, I've never heard of anybody that came in, in the industry who broke into a data center and really stole maybe a 3000 pound mainframe to get the data out. So, you need to balance all of this.

Ideally, you're going to have...like this example, encryption at REST all over the place but when you develop your security sometimes it's more important to get first encryption at REST on your laptops and then fix your firewalls and then look at other ways into the organization and this is what a framework is doing and HITRUST is doing this. It's looking at different levels of security that you need to get for PHI data, identifiable information versus de-identified information that has a different regime.

Gilad J. Kuperman, MD, PhD, FACMI – Director Interoperability Informatics – New York Presbyterian Hospital

Great, I appreciate that information that's very helpful, very interesting. I don't know much about that particular framework but I appreciate knowing about it.

My follow up question is, you know, let's assume that is a good framework, if you think about...and there are all kinds of stakeholders who kind of manage health data of various kinds, healthcare provider organizations, small companies, big companies, data aggregators, you know, and things like that, but, you know, I'm just thinking let's say from, you know, the point-of-view of a healthcare provider organization maybe, you know, medium-sized hospital or something like that. If they had to adopt this kind of a framework is it a, you know, a modest amount of effort, is it a, you know, significant amount of effort, is it a tremendous amount of effort?

I'm just kind of wondering, you know, from where we are now to, you know, moving into, you know, something more formal, a more formal security framework, you know, is it going to be easy, it is going to be hard, is it going to be very hard?

Andrei Stoica, MS, PhD – Vice President Global Systems Development & Security – IMS Health

Well, that's a hard question and the reason it's a hard question is because different entities are at a different level in protecting their data in having sophisticated IT operations. So, somebody that's not sophisticated does not have an IT department it's mostly outsourced, it's not going to be easy, it's something that they will need to have a chief information security officer that will define some kind of strategy to apply it. They will have to have a small staff in security to start looking at their operations to define targets for the operations either for the local staff or let's say you have a system that is outsourced, you have to tell providers. You can work without providers they actually are becoming more and more aware of the security issues but you have to request certain controls to be in place. There are offerings out in the market but again not...it depends on where you are.

So, I would say normal operations is somebody that in the past, I don't know five years, had invested into their IT operations. A lot of these controls are just good IT operations, good computer science approach. You are going to do backup on your machines, you're going to have firewalls, you're going to have antivirus on your desktops. Those are common sense operational controls that is you have an IT department most likely have them in place. In that case I would say maybe it's medium effort to get to a point in which you can say you are secure. If you don't have those in place then it's going to be hard.

Other companies that operate and I can give you examples of a lot of data integrators that's their business for them, and I operate in a company like this, for us it's going to be extremely damaging if we actually lose data. So, we took it upon ourselves for example to increase our security. So, we didn't wait for standards, we didn't wait for anything, we increased our security. For companies like this it's going to be fairly easy to look at this comprehensive framework and just add a couple of gaps here and there.

Gilad J. Kuperman, MD, PhD, FACMI – Director Interoperability Informatics – New York Presbyterian Hospital

Great, that's very helpful, thank you very much.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Do any of the other panelists want to comment on that line of questions that Gil just...

Ryan Andersen – Information Technology Consultant Network Administrator - Milliman

No.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Okay.

Denise Anthony – MA, PhD - Vice Provost for Academic Initiatives & Professor of Sociology - Dartmouth College

This is Denise.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Okay, Denise?

Denise Anthony – MA, PhD - Vice Provost for Academic Initiatives & Professor of Sociology - Dartmouth College

Yeah, I was just going to say that even the work on hospital compliance with HIPAA we did would just support entirely what Dr. Stoica just said that...and it's not just the sophistication of the IT system it's other aspects of the hospital infrastructure, the resources, the staffing, etcetera that is also going to have an impact on, I think, any kind of regulatory or even IT solution that's recommended. So, expecting, you know, a lack of uniformity across the country would be really good to expect going into it.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Well that begs a couple of questions on my mind but I want to see if I have some other Workgroup members queued up?

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Hey, Deven, this is Lucia, I have my hand up, but I know other people haven't had a chance yet.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Yeah, I don't...if people are using the hands up function I don't have the screen that lets me see it.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Oh, okay, well, my hand is up but I will defer to my committee members who haven't had a chance to ask questions yet.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Okay, I have one as well, but I'm in deferral mode for members.

David F. Kotz, PhD – Associate Dean of the Faculty for the Sciences – Dartmouth College

This is...

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Is there anybody who is waiting out there, otherwise...

David F. Kotz, PhD – Associate Dean of the Faculty for the Sciences – Dartmouth College

David.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Okay, David, go ahead.

David F. Kotz, PhD – Associate Dean of the Faculty for the Sciences – Dartmouth College

Yeah, I guess this might be a question for Ryan or perhaps the others. A month ago at an NSF meeting Latanya Sweeney was talking about this phenomenon of one's health data disseminating through a network of providers and data aggregators and insurers and so forth and she dreamed, in a way, of the opportunity for a patient or a person to be able to see not just this set of disclosures that were made by their immediate provider to some next person but eventually downstream, you know, where was that data, where did that data go and you can imagine maybe not that many people wanting to explore the full graph of data flows but some people might want to know where that data ended up. Is that feasible both technically and organizationally?

Ryan Andersen – Information Technology Consultant Network Administrator - Milliman

Yeah, I mean, it is, it might actually already be there it's just that nobody has asked for it. What we try to do...and I can just speak for what we do and what we've accomplished I guess, but most of the data that we get is, you know, it obviously starts at a provider and then it goes to an insurance company or a payer and then that payer typically that is where we consume data from the payer and so that payer can...so the doctor knows that it's going to, you know, insurance company "x" and then insurance company "x" knows that it's going to Milliman and then we at Milliman track everybody that's looked at it and so at least on that branch...now obviously there are going to be, you know, hundreds and hundreds of branches of, you know, different...it's going different places and things like that but I can...and, you know, we are, you know, towards the tip of the end and so I can say that we could tell a patient at least, you know, that...from that provider through that insurance company and through us we could tell that patient exactly that.

I understand why, you know, it would be a daunting challenge to say everywhere that it went because, you know, from my point-of-view it's pretty simple but, you know, I'm not the provider, but, you know, the provider is probably only going to send it to a few places as well hopefully and so from their point-of-view it might not be that difficult either. I think the onus is going to fall on the insurance...as of right now the insurance payer I think is going...it would be difficult for them but certainly achievable.

David F. Kotz, PhD – Associate Dean of the Faculty for the Sciences – Dartmouth College

Okay, good to know, thank you.

Andrei Stoica, MS, PhD – Vice President Global Systems Development & Security – IMS Health

And this is Andrei, I want to add to this. Technologically that's possible but an infrastructure to implement and track this is probably going to be extremely expensive. So, if you think of health information exchanges that infrastructure to put in place was not easy and we're still going through this and that is just to exchange the information.

To actually keep track of all the data that goes everywhere, yes, technologically possible you can tag it, you can put it into a directly and then the consumer or the patient can check it, but the complexity is going to be...and the cost to operate that is going to be very high.

In addition to that data gets aggregated and de-identified aggregated, so also you'll need that theoretical framework or thing of defining when does it stop being my data let's say, is it my data when I'm part of an account of a patient that for example had a visit to a hospital in Philadelphia area last week, is that part of me, my data or not. So, we need a framework, a theoretical framework to define what your data is as the data gets aggregated and that's going to become even more difficult to track. So, theoretically possible an infrastructure to do this is probably going to be prohibitively expensive.

Ryan Andersen – Information Technology Consultant Network Administrator - Milliman

This is Ryan again; I might follow up on my comment. I think that one way the theoretical framework might be simply to say, you know, where did that data go when you were the custodian of it and I think the framework resides then at each point that the data landed and so whoever, you know, was the custodian at that point they should absolutely already know where it went.

And so the framework is, I think, unless I'm mistaken, I mean the framework should already be there because if they're following current regulations the framework should be there it is just a matter of bringing those individual framework together, you know, you kind of have to go...like I said, go through the tree of where that data went and even if it's de-identified I agree with what you were saying there that at some point it is not really your data anymore you haven't shared any personal information specifically.

But you should...the framework should already be there for most of the people that have healthcare data. They should already know what, you know, what they've done with it, who has seen it.

David F. Kotz, PhD – Associate Dean of the Faculty for the Sciences – Dartmouth College

Okay, interesting.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Hey, Deven, this is Lucia, can I just ask a question about that last colloquial?

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Yeah, sure.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

So, can you guys talk or maybe clarify for me, because what I don't understand, and I did not hear Dr. Sweeney speak I was busy doing other things of course, tell me a little bit more about the ability, for example in Ryan's example, the custodian to say where it went in its identified versus de-identified state, right, so I know that, you know, aggregated data can be aggregated across suppliers in an identified way and then it can become de-identified whether that's expert or a safe harbor, TBD, but is it possible that...is it possible or appropriate we can have policy discussions here to keep track of where it's going once it's de-identified. I mean, de-identified as required by law.

Andrei Stoica, MS, PhD – Vice President Global Systems Development & Security – IMS Health

Sure, I mean and so let's go back. Identifiable information, yes you need to keep track of that one. What I was referring to is let's say Company A gets some DID or Entity A gets some identifiable information maybe this is an insurance claim processing and then they have to send it to a couple of business entities to do the processing so the data goes from Entity A to Entity B and C. Entity A of course knows what the data is and they will tag it and they would have a record of it but if you look, as a patient, what I need to do is go and check with all these entities where my data is so that's the infrastructure that at least I'm not aware that that's in place today so you can actually go and find a full list of where my data is. It's very similar with a health information exchange infrastructure that it took some time to be in place and it's still not there yet.

When it comes to de-identifiable information then it's even more difficult to track because that gets mixed and as part of other databases it has different security requirements. So technologically possible, yes, but it's something that it's probably not done today to actually track all the de-identified information and how that gets aggregated and used in different business processes.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Okay, great. So, one of the questions that I had, this is Deven, is back to the issue of sort of risk-based frameworks that are beyond the framework that already exists in HIPAA which already we know applies to some health data holders but not all health data holders and a recognition that I think a number of you put forth in your presentations that, you know, the risk is contextual and that we have a wide variety in the types of organizations that collect and hold and share health data so that, you know, a framework that might work very well for a well-resourced organization wouldn't work very well for one with smaller resources.

And I'd like to have each of you or at least those of you who are interesting in opining tell us what you think that means for setting policy around security in health big data and what should...what can consumers for example reasonably expect when their health data is in an environment that, you know, may or may not be covered by comprehensive law or if it is covered by comprehensive law there is still some wide variety and implementation and on top of that how do we make sure that frameworks that we instantiate in regulation can sort of keep up with where the puck is going from a security risk standpoint?

And so there are multiple facets to this question but the common thread is what's the best way to create some consistency, if it's possible to get it, around security, you know, through policy?

Andrei Stoica, MS, PhD – Vice President Global Systems Development & Security – IMS Health

I'll take that, this is Andrei...

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Deven, this is Lucia are you asking in general? Because we're really talking about big data here, right, this isn't a generalized hearing about HIPAA security writ large.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

No, it's about big data.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Okay.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

I mean, HIPAA has a piece of it because some of the big data, you know, some entities depending on how you define big data, are going to be HIPAA covered. So some of them are going to be covered by it and some of them are not.

But it's meant to sort of encapsulate the fact that we have, you know, a big world out there where there is a lot of health data and data with health implications growing and for which, you know, security questions come up and sometimes they're about adequacy of regulation and sometimes they're about, you know, how does regulation keep up with where things are going, what's the best way to set policy in such an ever changing and contextually rich space?

Andrei Stoica, MS, PhD – Vice President Global Systems Development & Security – IMS Health

This is Andrei, I'll take a first shot at this one and I do believe that this kind of approach should be very similar regardless of the subject in security meaning that today's big data tomorrow are you going to have microprocessor devices inserted in your blood that is going to transmit data wireless and, you know, use your imagination, the technology is evolving very, very fast.

So, if you step back to the basics what HIPAA does, and I do believe we need to continue along those lines, is setting out some outcomes, security objectives but those are the outcomes. You don't have the specifics because the specifics can change daily. They said that's the whole reason of using a risk-based approach because legislation like HIPAA is going to provide the guidance saying for example, you need to let's say de-identify information such that the risk of re-identification is small. Then what small is actually changes with technology.

I can tell you that the algorithm that we were using 10-15 years ago and the machines that you were using 10-15 years ago they were very secure back then but today they are not. So, that quantification of what a small risk is should be in a framework that evolves and that's the industry framework that I was talking about because that's based on a risk that you have to constantly re-evaluate. That's in my mind the connection.

So, when you look at the legislation the legislation should actually set the outcomes and then the specific standards which evolve, and I'm not exaggerating when I'm saying daily sometimes, those are the ones that actually set the specific measures the meet the outcomes of the legislation.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Thank you, other thoughts on this question if you have some?

Denise Anthony – MA, PhD - Vice Provost for Academic Initiatives & Professor of Sociology - Dartmouth College

Deven, this is Denise and I don't have any good thoughts other than that's exactly the right question, but I agree, I think, you know, the challenge...I wish I had solutions, I mean, I generally recommend and agree with the approach of the, you know, setting a floor with targets or goals that might be higher than that to achieve and I think in general that is sort of what HIPAA has done, the FIPS, you know, basically does that and then moving security and privacy by design principles I think go a little bit farther than that but, so, yeah, I don't have a good answer to your question, but it's the right question.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Can I ask a follow up question, Deven? This is Lucia.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Sure, go ahead.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

I had a question for Andrei and Ryan written down kind of about this so I'm going to...so it seems, from what you guys said, that there is a little bit of a correlation, and maybe this is two-part question, between the ability of an organization to address security in a sophisticated way and its size and resources.

So, for first question is, is that, you know, a perfect correlation, is it small organizations could do it if they put their resources into it or is it really...I mean, you know, are we really talking about a size matters and if size matters is there some...is there a policy indicator here relative to not just a functional outcome and a floor but a capabilities floor, you have to be capable of doing this, this and this to have the ability to use data in a particular way? Is that something we should be considering?

Andrei Stoica, MS, PhD – Vice President Global Systems Development & Security – IMS Health

I think there is a capability floor here and there is a step function in here. So, if you have a small organization of 10 people then it's going to be hard, it's going to be a huge impact for you because you're going to hire five people 50% of your organization you need to increase to deal with security.

Now if you go to large organizations then it doesn't scale in the linear fashion. It's not like you're 1000 people organization then you need to hire 5000 people in security.

So, there is a step function in here and in very small numbers, yes, there is a huge impediment and huge cost differential for security but as you go to a path to critical mass and you have a decent sized IT operation that will deal with structure, IT processes then it becomes easier and easier, you don't have to have a small army in security.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Thank you.

Andrei Stoica, MS, PhD – Vice President Global Systems Development & Security – IMS Health

Did I answer your question? That was the second question, I'm sorry, so this...

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

The question was whether there is a capability floor and the first one was kind of like how much of a correlation is there between size and capability just, you know, I know you're guessing and it probably hasn't been studied, you know, in a definitive way, but, you know, you're a pretty experienced guy, so guessing, how much of the capability is there?

And the reason we ask that is because if we really have a learning health system we want people who need to be able to learn in a secure environment, we have to figure out where those two things meet.

Andrei Stoica, MS, PhD – Vice President Global Systems Development & Security – IMS Health

So, the correlation...

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

...Pardon me?

Andrei Stoica, MS, PhD – Vice President Global Systems Development & Security – IMS Health

So, the correlation is that in small organizations I would say maybe total revenue in double digits millions, 10, 20, 30 million dollars there is a strong correlation between capability and size just because the cost of security is a significant percentage of the revenue.

As you go to triple digits in the millions then you actually start seeing organizations that have invested in this, again, it's hard to estimate, but in my experience companies that start having 50, 60 million dollars in revenue and above you're going to see structured processes, you're going to see functions like chief privacy officer, chief information security officer, security teams they start showing up.

I'm not saying that small organizations they don't have it, the responsible ones they probably do but you see a huge differential in cost and unfortunately I've seen organizations, small sized, that due to cost reasons they don't invest in teams for security and for privacy.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Great, thank you. Other questions?

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

I actually have another one Deven, I'm full of questions today, but again, I want to defer to other people so they have a chance.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Yeah, if you've done the hand raise function I won't be able to see you so speak up. Okay, Lucia, it's all...keep going.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

This is for Ryan and maybe for Andrei, but I was wondering if you could talk a little bit about, you know, sort of in the data technique that you guys apply to the data particularly to aggregated datasets, could you talk about the difference about what's in the data as your processing it versus what's in the information output that you disclose to whoever your customer is?

Ryan Andersen – Information Technology Consultant Network Administrator - Milliman

Well, sometimes there is no difference in so much as they, you know, they want the detailed information that they've sent us available through our interface for them to do, you know, data warehousing decision support system type of work and so sometimes there is no difference at all other than...

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

And so that's a reflection back to the covered entity that gave it to you in the first place to use the HIPAA structure?

Ryan Andersen – Information Technology Consultant Network Administrator - Milliman

Correct.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Okay.

Ryan Andersen – Information Technology Consultant Network Administrator - Milliman

Now the other types...there is additional information in there and, you know, some of the aggregation and some of the, you know, the Milliman propriety knowledge that we apply to the data and then, you know, we group it up and give them different things also.

There are other entities that we work for that when we do give it back it is a much...it's de-identified, it is not available at a detailed level and so we're just looking at things like, you know, we're looking at things like trends, we're looking at things like, you know, aggregation rollups and so it really does vary as to what it is that we're asked to do. But, you know, the people that are asking us are the owners of the data in our eyes and so we are...we're, you know, kind of doing their bidding if you will.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Okay, so, just one follow up question maybe Andrei has a different answer, so in this last example that you just gave where it's not, you know, directly back to the particular covered entity, does it have health indicators in it or is it like numerical and statistical in nature?

Ryan Andersen – Information Technology Consultant Network Administrator - Milliman

There can be health indicators in it, yeah, certainly.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Okay.

Ryan Andersen – Information Technology Consultant Network Administrator - Milliman

There are, you know, we have safeguards in place to make sure that it's not identifiable health indicators, but yeah, absolutely we do, you know, different rates or evidence-based measures are one of the things that we do that, you know, how many people have high blood pressure or how many of them are on high blood pressure medication as compared to how many are...that have high blood pressure and so there are things like that which we've taken precautions that it's not going to be...you can't find out that Ryan Andersen has high blood pressure. Does that answer...is that the correct...

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Yeah, that helps me, you know, sort of picture it in my head and I don't know if that's helpful for other Workgroup members but it's definitely helpful for me to picture in my head what's being made from this information, we're taking information and we're making something out of it, what are we making.

Ryan Andersen – Information Technology Consultant Network Administrator - Milliman

In our case a lot of times they're making decisions or they're making, you know, business objective decisions. So, if they're finding out that their medical management team isn't doing a very good job of managing people with diabetes some of the things...some of the indicators, some of the information that they're going to get from our data aggregation efforts are going to help them, you know, go and create an objective, like, you know, we need to do a better job of that and then plan out how to achieve that and then through the continued use of this data aggregation they're going to be able to see those rates change over time if their efforts are successful. That's just one example.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Okay and Andrei did you have anything you want to add to that?

Andrei Stoica, MS, PhD – Vice President Global Systems Development & Security – IMS Health

I agree with Ryan this is this is the typical use when the data does not...the results don't return to the data owner, in fact, even when they return to the data owner. What people are looking for is business intelligence. So tell me why this process is not working or tell me how I can improve this or tell me what's the outcome of this. So you have some kind of health indicator but the focus is not on patient ID that's not needed in the industry.

What's needed is, to Ryan's example, why...how does a patient...how is a group of patients going to react on this medication versus other medications which one is more effective. Those are the indicators that are needed in the industry and big data companies are in the business of processing some of this.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

And Deven, I think exhausts my list of questions.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Okay, well that's good because I think we're almost out of time. But they were good questions, Lucia, thank you. Was there anybody else who wanted to ask a question of our panelists?

Okay, well, Andrei, Denise and Ryan thank you so much for your willingness to talk to us today. I think it very could be that as we go down the pathway towards coming up with recommendations in some of the areas that you've talked about that we may come back to you with some further questions, but you've definitely given us some terrific food for thought to get us started and we greatly appreciate it, thank you.

Ryan Andersen – Information Technology Consultant Network Administrator - Milliman

Thank you.

Denise Anthony – MA, PhD - Vice Provost for Academic Initiatives & Professor of Sociology - Dartmouth College

Thanks.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Okay.

Andrei Stoica, MS, PhD – Vice President Global Systems Development & Security – IMS Health

Thank you.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Now for the rest of the Workgroup members don't go away we're going to try to use the rest of our time on the call, even though we don't have much of it, to see if we can continue to make progress on the consent topic that we were doing a deep dive on during our last phone call.

Oops, didn't mean to go quite that far...so just, you know, to review we sort of organized the thoughts here to sort of draw a line between, you know, entities that are covered by HIPAA where at least in that environment we have some rules about when consent or a patient's authorization is going to be required in order to access and/or disclose data and then, you know, the context outside of HIPAA where the rules are a bit less clear where companies, at least in the for profit sector, can be held to commitments that they make to consumers with respect to how their information is used and what sorts of uses will require additional consent or authorization but that generally it doesn't have the sort of same structure as would be required in the HIPAA environment.

And really, you know, even within the HIPAA environment to date we have sort of focused on the research use case and whether HIPAA and Common Rule requirements appropriately advance innovation in the learning health system while still building trust and protecting individuals for patients and the consumers.

And some of what we've talked about is whether low risk research or what we would bucket at low risk research could be acceptable to do without necessarily needing to get consent or authorization, or even a waiver from an IRB and what would determine what constitutes low risk if we were in fact comfortable drawing such a line in a recommendation.

And we've also talked a bit about, but not in detail yet, about what the role of transparency is in the place of consent such as in circumstances where the usage of the data is reasonably appropriate given the context. And that we might also sort of bucket these in the sort of low risk uses or research uses category as well.

But since we've focused a lot on research issues it does beg the question of whether there are other use cases within HIPAA that might need further discussion or in other words, you know, really how much of the HIPAA universe do we think we need to take on in order to deliver a set of recommendations on health big data that help us to make sure that the opportunities that arise with health big data can be appropriately leveraged when that data is held by entities that are covered by HIPAA.

And then when you think about outside the HIPAA framework, again, as we talked about, you know, there are some rules that govern here, certainly the Federal Trade Commission's authority with respect to for profit companies, also, you know, some other regulatory regimes that might apply, but generally we haven't done as much thinking about consent in this environment nor have we thought through whether there are some lessons learned from HIPAA that we might borrow in terms of recommendations for the non-HIPAA environment.

For example, should consent requirements attach to those uses and disclosures that are outside of what should reasonably be expected given the context, this is consistent with reports that have come out of the FTC on issues of consumer privacy generally and if we follow that line of thinking do we think that there is enough understanding of context among people out there or does that really get to how you define context and is there and is it possible to use sort of a low risk/high risk risk-based framework for the policies in this context as well and what would that look like if we went in that direction.

And again, recognizing the data that relates to health as an ever expanding list which could pose challenges to placing more stringent requirements on the sharing of "health data" but doesn't necessarily...but perhaps following more of a risk-based framework and having some conception of what risk means maybe that suggests that we don't have to define what health data is or isn't if we're looking at what the risks are for consumers with respect to uses of personal data.

So, that's just trying to, you know, sort of summarize where we've been and on top of that, you know, there might be some overarching issues that are in play in both the HIPAA and the non-HIPAA environment, lots of concerns raised on our last call about "all in" or "all out" which doesn't really give people very much choice. But do we have a policy environment and technical capabilities to honor those policies that are mature enough to at least, at this point, enable much granularity.

How can consents be persisted across environments, you know, we know from our deeper dives on some of the laws that some of them come with re-disclosure prohibitions, the substance abuse, federal substance abuse treatment rules are an example of where, you know, if you are required to get authorization to disclose it once the entity to whom you've disclosed it is similarly required to get authorization in order to disclose it further but not all the laws are written this way and so some...so an entity that does business in the State of California for example and might be accustomed to dealing with some more granular consent requirements might send data to a state that is a HIPAA only state and to an entity covered by HIPAA and those requirements do not exist. So, what does that say about the, you know, whether consents need to be persisted or whether they should be persisted and then if the answer to that is "yes" how do we do that.

And then a recognition that consent puts the burden on individuals, so it can't be the sole or primary protection really in either environment but at the same time, you know, there is a lot of appeal to giving people choices to begin with and allowing them to be able to do what they want to with data where they have the authority to consent including sharing it really broadly if that's the way...if that's what they want.

So, with all of those observations, you know, Stan and I the staff from MITRE and our support staff from ONC and our support team from MITRE have been trying to think about how to tee up some recommendations for the Workgroup and, you know, keeping in mind that, you know, what we say about this issue can be both a combination of both findings and conclusions as well as actual recommendations for moving policy forward and so, you know, we have a couple...we've identified one around research uses in the HIPAA environment and whether we're comfortable as a group reiterating or refining our initial recommendation that we made back when the Advanced Notice of Proposed Rulemaking came out about re-use of clinical or claims data and where that's done to contribute to generalizable knowledge and you're doing it as a covered entity in a controlled environment that we should treat that more like operations necessarily than research. But are there caveats to that and how would that get implemented and then consider whether there are other use cases under HIPAA that we would want to deal with.

And then we've tee'd up, you know, really more questions than straw recommendations in the non-HIPAA environment because we just haven't had as much of a chance to talk about this and frankly we're not going to be able to do that on this call either because we're running out of time, but when is it that consent should be required and are there factors that come into play that we could at least articulate as being ones that argue for people to have choices and ideally ones that are more granular than all in or all out.

So, I'm going to pause for a minute and ask Michelle to queue up the public question line not because we're moving to public comment quite yet but we want to give people more time to get in the queue if they have a public comment to make. So, we'll pause for a moment for that to happen then we'll come back and have a bit more reaction to at least the framing of the consent issue from Workgroup members and then we'll move to public comment.

Public Comment

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Thanks so much for remembering, Deven. Operator can you please open the lines?

Caitlin Chastain – Junior Project Manager – Altarum Institute

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. If you are on the phone and would like to make a public comment please press *1 at this time.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Okay, that's great, we can leave this slide up so people can see it. So, the Workgroup members have all had the slides circulated to them. But I want to get some reaction to the framework. I think I'm...again, we don't have very much time so my apologies for that. We always invite sort of off line thoughts on this particularly when we run out of time on our calls so we can continue to make progress during our public calls.

But one question that we may be able to get some feedback on is whether we want to take on other big data use cases in the HIPAA environment beyond the one for research given that we have a comprehensive regulatory framework that exists in HIPAA already.

And, frankly, I would argue for taking on...focusing on the research uses, because of the sort of opportunities and potential to contribute to the learning health system as a sort of primary goal in an environment where we already have a, you know, an existing regulatory framework for all sorts of uses.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

And Deven, I just wanted to...this is Lucia, that's...your question relates to the straw person recommendation on slide 10 correct?

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Yes.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Okay, got it.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

It was also I had a...rather than invite feedback on the straw recommendation which is a research use case it was more about, you know, whether there are other use cases that we would take on other than research. Am I still not being clear?

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

I'm dense today because it was a long weekend and I'm...

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Oh, no, I'm...

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

And I was just looking for something to read and respond to but it's okay.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

No...

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

I'm going listen along and defer to other people, because, you know, I have my own opinions here.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

I'm just saying that as a default in a HIPAA environment we have HIPAA which has, you know, sort of guardrails and rules about, you know, what you can and cannot do with data and for what types of purposes, right?

We've talked about and had testimony about how the way that HIPAA regulates research maybe a place where we might recommend some tweaking either of Regs or through guidance in order to facilitate uses of data...

Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP

Right.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

For learning health system purposes. Is that the only sort of big data type of use case that we would want to take on in our examination for HIPAA covered entities?

Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP

Deven, this is Stan; I...you know, this is an area I think we're going to have to get a little more exploration around it. I think we do need to consider...I think our remit was a little broader than just research because there is, you know, the sharing aspects certainly when the patient requests themselves and making sure that data can flow more but that whole treatment aspect of, you know, what sources of big data can be utilized and passed back and forth in an exchange environment.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Okay, all right, fair enough.

Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP

I mean, again, we've talked mostly about the research side but I'm not sure that's what we're limited to.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

I don't think we are. I'm suggesting that we figure out a way to limit what our scope is, that's all I'm saying.

Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP

Right, I hear you, okay.

Micky Tripathi, PhD – President & Chief Executive Officer – Massachusetts eHealth Collaborative

And Deven, sorry, this is Micky, were you suggesting limiting it for the purposes of practicality and just to...

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Yes.

Micky Tripathi, PhD – President & Chief Executive Officer – Massachusetts eHealth Collaborative

You know sort of take one step at a time? Okay.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Yes.

Micky Tripathi, PhD – President & Chief Executive Officer – Massachusetts eHealth Collaborative

Yeah, I mean that makes sense to me. No big principle behind it for me.

Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP

Right. One step at a time is different than if that's all we're going to consider, I mean...

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Well, so, but I want you to think about that. I want you to think about we're only on the second deep dive of like six areas that we have...

Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP

Yes.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Explored and we have a non-HIPAA environment as well as a HIPAA environment for the deep dives.

Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP

Okay.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

So, I guess I'm just suggesting that I think it would be incumbent upon us to think about what are the most important opportunities we want to leverage for health big data and for us to limit our exploration.

Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP

Right.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Particularly within the HIPAA governed entities.

Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP

So, what you're talking about within HIPAA it's the research and then we can explore the other non-HIPAA environment further.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Well and you laid a couple of others on the table which I...

Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP

Okay.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Wasn't foreclosed to thinking of them. I'm just suggesting that we not take on the whole universe.

Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP

Yeah, yeah, okay and I agree that as I think about it we have the HIPAA environment, we haven't even turned really to the non-HIPAA environment very much yet.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

Yes.

Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP

And I think that is also important.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

All right. So, we won't be able to sort of close that debate off either, but I want you guys to think about that because now that we've got people queued up presumably for public comment we need to give them a chance.

Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP

Okay.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

So, okay, never enough time on these calls. All right, so we're ready.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Well, thank you, Deven, we actually don't have any public comment, but I appreciate the extra time for people to provide it if they wanted it.

Deven McGraw, JD, MPH, LLM – Partner – Manatt, Phelps & Phillips, LLP

And we'll do this every meeting now and people will get accustomed to having more time and hopefully we'll get some more public comment. So, sorry I had to cut that all off folks, but I hope that those of you who were able to listen in on the Policy Committee and Standards Committee meeting tomorrow to hear the reports of the interoperability roadmap because we'll be getting pieces of that as sort of our next work stream. And any inputs you want to provide on the conversations that we had today in the interim will be most welcome. And with that I think we're done.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Thanks so much Deven.

Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP

Thanks, Deven.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Thanks, as always, Deven.

W

Thanks.

Stanley Crosley, JD – Director, Indiana University Center for Law, Ethics & Applied Research (CLEAR) in Health Information – Drinker Biddle & Reath, LLP

Thank you.

W

Thanks.

M

Thank you.

W

Thanks, all.