



## HIT Policy Committee Privacy & Security Workgroup Final Transcript January 12, 2015

### Presentation

#### **Operator**

All lines are now bridged.

#### **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 McCallie?

#### **David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Here.

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

Hi, David. Deb Bass? Donna Cryer? Gayle Harrell?

**Gayle B. Harrell, MA – Florida State Representative – Florida State Legislature**

Here.

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

Hi, Gayle.

**Gayle B. Harrell, MA – Florida State Representative – Florida State Legislature**

Hi.

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

Gil Kuperman?

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

Gil Kuperman here.

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

Hi, Gil. 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. Helen Canton-Peters, sorry ONC staff. John Wilbanks? 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? 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.

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

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

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

**Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology**  
Hello. Mark Sugrue? Micky Tripathi? Stephania Griffin?

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

**Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology**  
Hello and Taha Kass-Hout? And 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. 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 Lucia Savage?

**Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology**  
Yes, I'm present.

**Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology**  
And I think that's everyone. So, with that I'll turn it back to you Deven.

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

Okay, great, thank you very much Michelle I'll extend my apologies on behalf of our Co-Chair, Stan, who got caught up in a little bit of weather disrupted travel this morning so he's not able to join us on this call. I promised him I would get him back by requiring him to take on the lion's share of another meeting, but hopefully he will have safe travels most importantly.

So, welcome everyone to our first call of 2015. I hope you all had very good holidays and Happy New Year. We are excited to sort of kick off our discussion on the big data topic that we began to take on at the...in hearings in December. If I could have the next slide, please?

So our agenda today is to talk a little bit about how our plans for meetings in January and early February with respect to this issue and then we'll go through some slides where Stan and I, and the staff try to summarize some of the key themes that came out of the hearing focusing really on the concerns that we heard raised and then what we hope to do is to make sure we've sort of got all of the sort of key themes and concerns at least, while not maybe perfectly wordsmithed on these slides, at least represented in our materials, because our goal is to ultimately start ticking them off and diving into each one of them in some more detail in subsequent calls. And so if we're able to get started on one of those today we've tee'd up the issue of health data de-identification as our first topic.

And as you may have noticed, if you had time to review the slides before the call today, there are some summary slides on the hearing testimony that begin at slide 19 in the deck and those are there for your edification.

We also sent out to Workgroup members the initial draft transcripts of the hearings, of course Altarum will be cleaning those up and making public versions available on the Health IT Policy Committee website soon, but given that we're starting these discussions in advance of those being completed we did get out to the Workgroup members an early version of the transcript.

But the summary slides, if you haven't had time to read the transcript should at least tide you over until you have an opportunity to read through the transcripts and we also circulated some of the written materials that some of our presenters sent to us that specifically mentioned or spent time discussing the issue of de-identification, which again we hope to sort of drill down on today. So, does anybody have any questions about the agenda?

Okay, let's move to the next slide then. We're on slide three for those of you who are following along, now we're actually on slide four. So, in terms of our work plan we have our meeting today where we're going to start diving into what we learned in the hearings that we held in December and then we have another call on the 26<sup>th</sup> where we will do more of the same, and another call on February 9<sup>th</sup> where we will continue our discussion, hopefully diving into as many topics in more deep detail as we possibly can.

And then it's likely that we're going to need to make a transition to discussing some aspects of the interoperability work plan for the rest of our calls in February which I think is only one more. We do tend to typically have scheduled some time to at least report on our progress to the Health IT Policy Committee. I think we will not likely be done with this issue by March 10<sup>th</sup> but we do want to begin bringing the committee as a whole into the conversation that we're having as a Workgroup and so we've slotted a goal to at least begin talking to them about what we've learned, what we're thinking even if we're not...we won't be fully prepared to do actual final recommendations by that date.

And then as soon as we're able to return to this topic, after completing work on the draft interoperability roadmap during the public comment period, we will do so. Does anybody have any questions about the work plan or the schedule?

All right, terrific. Next slide, please. So, again, as I said at the outset what we're going to do today is talk about some of the key themes that arose from the hearings or listening sessions that we had in December and they're very much focused on the concerns that we heard that this is not to say that the important testimony that we got on the potential benefits of health big data was not worth documenting or talking about. I think it is worth talking about and there are threads of what we heard from the testimony on benefits of big data in those summary slides and certainly any report that we would do to the Policy Committee I think we would want to talk about what we think the benefits are of health big data both for learning health systems and beyond.

But I think the concerns are what are going to take the most amount of thought from our Workgroup and where we need to spend a little time drilling down on, you know, what recommendations we would have to try to address some of those concerns in order to leverage the opportunities that we see in health big data.

So, we have not specifically tee'd up, you know, rhetoric and slides around the opportunities but, you know, unless someone...one of you tells me that you don't think it's worth even talking about, which I would be surprised, but of course am happy to have the dialogue about that, I think that any report that we make that comes out of this effort that we're undertaking as a group needs to of course talk about where we see some of the opportunities.

And so certainly, as we start to coalesce around some common recommendations and as we build towards developing the text of all that we want to say about what we've learned through this process we will need to build in discussions of where we think the opportunities were and we will have draft language on that for you to review and evaluate, and provide us with comments. Does anybody have any concerns about that thought?

Okay, either you are all on mute or I'm just...I'm going to assume everything is okay if I don't hear otherwise. Okay, next slide, please.

So, we start, we're on slide six, with thinking about what the scope should be of our examination of health big data, you know, keeping in mind that we heard an awful lot from some of the people that gave presentations to us and submitted materials to us on a whole scope of issues that arise with the collection and use of health big data in particular for analytics purposes.

And Stan and I propose that what is in scope for us, since we are the Privacy and Security Workgroup, are concerns that are related to privacy and security and that includes potential harmful uses because whether you think they're separate from privacy or connected to privacy often times when people express concerns about the privacy of their personal information, and health information in particular, many times it is about concern about what people will do with that data that could harm them.

So, we've put potential harmful uses in scope for us to talk about because they are so closely connected with the interests of individuals in protecting their privacy and confidentiality of their information.

What to us seems to be out of scope were issues about data quality and data standards, not that those are not important issues, but to the extent that they are not tied to privacy and security, which is the remit of our Workgroup, the recommendation from Stan and me is that we should consider those to be out of scope.

On the issue of non-representativeness of data Stan and I have proposed that this is out of scope and you may remember from the presentations that this is about the fact that sometimes the sources of data are not necessarily balanced in terms of what subpopulations are in that data, are contributing that data, are collecting that data and this may be particularly true outside of the HIPAA scope where, you know, you've got consumers gathering and using data on line where, you know, certain subpopulations may not be very well represented in that data.

And we've sort of put that as out of scope because it was our initial thought that, you know, we're not trying to resolve this from the stand-point of necessarily recommending ways to increase the representativeness of the data because that goes to the validity and replicability, and usefulness of any analytics or ways that you use the data, but certainly it's worth discussing in terms of its impact on privacy and security concerns as well and that includes the harmful uses of the data.

So, does anybody have any comment on where Stan and I are proposing to draw the line with respect to what's in scope for our conversations about this and what's out of scope?

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

Deven, hi, this is Micky Tripathi, I think the scope parameters make sense.

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

Okay, thanks, Micky and glad to have you on the call.

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

And this is Kitt; I agree otherwise it will just get too unwieldy thinking of topics without going into that other detail.

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

And Deven, this is Lucia; I think that it's a really good line drawing because it helps us draw lines that are specific to healthcare versus more generalized to all kinds of big data issues.

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

Right, right. Is there anybody that feels like something is in the out of scope category that doesn't belong there? Okay, good, it doesn't sound like it.

All right, so let's move onto sort of discussing the next slide, which is slide seven, beginning to sort of call out, again the key themes of the testimony in terms of concerns that we heard with respect to health big data and they can be grouped at least in the way that Stan and I, and the staff have conceptualized this, but of course this is up for discussion for all of you.

We've bucketed them into three bigger buckets with some sub-buckets within those. So, one would be the legal landscape and there are two pieces to that, one being, you know, the gaps in privacy and security protections for health big data, so you could call them gaps or maybe even under regulation.

And then you have a...you know, we heard some testimony about, you know, maybe the regulations are not necessarily a good fit either because they arguably create some disincentives for analytic uses of health data or because they create complication with respect to multiplicity of laws such as the issue of having multiple state laws to contend with when you're trying to do analytics using data from institutions in multiple states and so there are sort of two aspects to that.

And then there is the big bucket about, you know, some concerns about the tools that are commonly used to protect privacy, de-identification, which is something that I hope we'll have time to begin a deep dive in on the call today. When is patient consent required versus when can you depend on what patients reasonably expect from a particular type of data collection, norms of use types of issues. Transparency about uses of health data. Collection use and purpose limitations and how viable are they in a big data environment and data security.

And then the third big bucket is the one about harms. What are the potential harms and how do we prevent or limit, or redress them.

And so the next set of slides is really where Stan and I, and the staff really tried to add in some additional details about, again, this is about what we heard from our listening sessions and what we received in terms of written submissions from the people that we invited to give us some feedback. Next slide.

And so what I'm going to do here is go through these slides, I'm going to pause...I'm going to plan to pause rather than, you know, just talking myself for 12 slides, which I'd prefer not to do, I'm probably going to pause after each sort of subtopic area and begin to gather some input and what I'm hoping to get from you all today is not necessarily wordsmithing, we will, of course, need to articulate these to the committee in the way that we want to have them articulated.

But I'd like to use our calls not for wordsmithing necessarily but to identify sort of big issues that were missing or if it's not just a mere wordsmithing issue in terms of, well, I can give you a better way to say it, but if you think that the wording is just really off and doesn't even really capture the concern very well, then those are the types of sort of bigger picture issues within these buckets of concern that I think we should spend, you know, the precious time that we have available on these calls to try to address making sure, you know, at this very early stage in our discussions that we really got it all out on the table so that then we can sort of chunk it up and parse it out and do deeper dives on it in subsequent calls.

So, with that, you know, the first several slides deal with this, you know, the bigger topic of the legal landscape here and this first slide is really devoted to uncovering what some of the gaps are or really potential under regulation with respect to privacy and security.

And we know that HIPAA applies in some cases on the first bullet point on slide eight but only to identifiable health data when it's collected, accessed, used and disclosed by some, in other words, covered entities and business associates, it's not a data protection law, it does not apply to health data that's collected, accessed, used and disclosed elsewhere, outside that HIPAA bubble, which includes consumer facing or consumer marketed devices and spaces such as the web and mobile Apps, that's not the only non-HIPAA covered space but it is one that was highlighted in the presentations that we received.

In addition, you know, non-health data if collected and used maybe initially for non-health purposes would also likely be outside of the scope of HIPAA, again, depending on who is collecting it, we may need some wordsmithing there. But it could potentially be used for health purposes and this is our articulation of sort of what we heard from a lot of our witnesses that, you know, potentially all health data could, depending on how you were using it be construed to be health data.

The Federal Trade Commission has authority both for entities that are subject to HIPAA and those that are not to crack down on unfair and deceptive trade practices with respect to health data and non-health data collection and use.

**M**

Oh, hi, how are you?

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

Okay, so, I think that was not meant...assuming I'm not being interrupted by a question, make sure you're on mute if you're not speaking. Thank you.

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

We're looking for it too Deven, thanks.

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

Thanks, keeping us on our toes here. But the kind of authority that the FTC has while certainly very helpful and important and I think if you talk to any companies that have been subject to enforcement actions by the FTC they consider it to be quite serious. So it is something to take into consideration but it isn't the kind of comprehensive privacy and security regulatory framework, you know, that those of us who are accustomed to dealing with HIPAA are certainly accustomed to or that apply within that HIPAA bubble.

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

Deven, this is Lucia, I have a question/comment just as we develop this information.

**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**

So, something we should probably clarify is whether the FTC's authority reaches to non-profit organizations. I know that on the competition side it does not. Because big health data doesn't always happen in a for profit environment.

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

Right, right, right that's a very good point Lucia we'll make a note to clarify that. And then the last bullet point on this slide is with respect to the ability of consumers and patients to have access to health information held by entities that are covered by HIPAA but they often have difficulty exercising this right either at all or in a timely way. This right does not extend to all personal data that a consumer or patient may collect and share.

Consumers also don't have access to information use to make decisions about them other than in circumstances that may be covered by the Fair Credit Reporting Act and often don't have access to research data. This came from the testimony that we heard from some of the consumers and patients that we asked to address us.

So, this is the slide on gaps from the under regulation side of that issue. The next slide deals with the, you know, the other side of that coin regarding over or mis-regulation and so I want to make sure that we've got sort of everything accounted for in terms of the concerns we heard about not enough regulation here.

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

Deven, hi, this is Linda Sanches.

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

Hi, Linda.

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

Hi, I just wanted to make the point that of course consumers do, under HIPAA, have the right to get access to information used to make decisions about them.

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

Right.

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

So, when we're thinking about how to respond to this point, you know, it might be a regulation where the provision is not being fully implemented or it may be perhaps not fitting in certain environments but not that it's not actually required by law.

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

Right, right that's...thank you, Linda and that's a perfect kind of...because that's not a wordsmithing comment it's a, you know, we don't have it really accurately captured here, that's very helpful.

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

Thank you.

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

Deven?

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

Yes?

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

Hi, this is Micky, I don't know where this would belong but I don't know if it's under regulation, is there something separate related to the fact that when, you know, the HIPAA definition of identified is very specific and once you go through the process of de-identification according to HIPAA then you can do whatever you want but there are many, you know, Latanya Sweeney's work and others, that suggest that that's not enough.

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

So, you know, interesting, we've got that...because we also tee'd up de-identification as a specific topic that we were going to discuss today...

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

Yes.

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

I think we probably omitted some of that discussion, in fact it does look like we omitted some of that discussion in these summary slides which we, you know, when we get to the topic of de-identification, which again, I hope we get to today, let's make sure we've got that captured.

But we may also, again, as we sort of throughout our process of digesting this material and beginning to come to recommendations we're going to be building essentially our letter that will go to the Policy Committee and, you know, it very well may be that we'll need a section that, you know, does go through all the concerns and we want to make sure that those concerns on de-identification, which we didn't include in these summary slides, again, probably because we had tee'd it up for specific drill down, we'd have to include that that's a very good point.

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

Right, okay, sure, yeah, because you can see it as a form of under regulation or to your point under de-identification a separate category.

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

Right.

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

You know wherever you think it fits best.

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

Right, right. Well you'll see when we get to those slides that we tried to sort of exhaustively mine that topic but you guys are going to let us know if we did.

All right, well let me move onto the next slide, which is the topic of what we've sort of for now labeled as potential over or mis-regulation the flip side of the legal framework topic.

And we just have two things on here so it will be interesting to see if we missed something, but one being the issue that was brought up on our legal panel about whether you continue to call it the HIPAA paradox or we find some other way to refer to it, but the distinction between quality improvement and research within HIPAA meaning that if you've got a study that you're doing for quality improvement and population health purposes it could fall under the definition of operations if the primary purpose of why you're examining the data is not to contribute to generalizable knowledge while, you know, if you're essentially doing the same study but you are intending to contribute to generalizable knowledge it's going to be treated as research and regulated more stringently and what does that mean for the ability...for encouraging people to sort of do analytics and share what they learn with the broader population.

And again, we'll have an opportunity to drill down on this but we've right now sort of surfaced it and it's probably wrong to call it over regulation but it may be a piece where the regulations or guidance related to how you interpret those regulations may need some additional work.

And then we've also bucketed in this category managing state information, health information privacy laws, which become an issue when you are trying to access data from data holders that exist in different states where those laws may apply. Thoughts on this?

**Gayle B. Harrell, MA – Florida State Representative – Florida State Legislature**

This is Gayle, I just would like to comment especially on the state regulations that unless there is some overarching federal legislation there is no other way to get around that and most states do have specific privacy and security regulations and they vary state to state as we heard.

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

Yes.

**Gayle B. Harrell, MA – Florida State Representative – Florida State Legislature**

And that will take more than just guidance I think that takes federal legislation.

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

Yeah, no without a doubt, Gayle. You know the guidance is really more potentially applicable to that first bullet not to the second. And so glad that we have you as a state policy maker on our group to help us think through what if anything we can and want to say about this second bullet.

**Gayle B. Harrell, MA – Florida State Representative – Florida State Legislature**

Yes, happy to be part of it.

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

Deven, this is Micky again, do we want to include Title 42?

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

The Common Rule?

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

No you mean Part 2, Micky, 42 CFR Part 2 for substance abuse treatment?

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

Yeah, yeah, sorry.

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

This is Lucia, so, I mean, I think what we were trying to do was sort of distill things that maybe were more surprising. I think a lot of people are aware of Part 2. The interesting thing about Part 2 or other federal laws compared to the state law issue is, they don't vary by jurisdiction Part 2 is Part 2, is Part 2, Part 2 whatever state you're in.

Similarly, if you have special rules that apply because of military situations or, you know, privacy act for federal health data all those things are the same in every state. And that's really what we were trying to tease out not that there are not special rules for special conditions but that as a result of the way state law operates sometimes the special rules for special conditions themselves vary.

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

Yeah, no that makes sense, I guess I was just thinking of it in the context of, you know, there is sort of...there is a paradox with CFR 42 as well in that the regulation applies based on the source of the data not in the content of the data so you get into a conundrum when you have data that wouldn't otherwise be considered sensitive just like vitals, but the fact that it came from a federally subsidized substance abuse provider all of a sudden puts it in the CFR 42 trap.

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

Correct and that's how people have interpreted it historically.

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

Yeah.

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

Right.

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

Yeah, no, I think that we're a little under...we probably...we should I think...you know, if we're going to call out the way that, you know, having different state laws can sometimes create hurdles to get through in order to have analytic uses of data, you know, we've got some other federal laws that we could mention as well.

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

It's an interesting irony Micky that you're pointing out it's sort of like the irony that, you know, we have rules related to quality of care that derive from acute inpatient facilities even though the care they're actually seeking to regulate now occurs in ambulatory and ambulatory-surg centers.

So, we sort of have this historical habit of doing things by location and obviously to achieve total computability in your ideal world you would have concepts connect to codes and as codes evolve the mapping would evolve, but I think that's probably fruit that's not even in our bowl to take a bite of that apple right now.

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

Yes.

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

But in terms of sort of...we did have presenters who talked about this and so we've got a bit of an under description problem I think with respect to this particular aspect of the legal framework question.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

And Deven, this is David, in our older Privacy Tiger Team discussions when we discussed HIPAA and the Common Rule didn't we identify other places where there is either confusion or overlap with the Common Rule? It seems like this quality research distinction is not the only one.

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

So, that was part of the...you know, when I went back to prepare for my presentation during the listening sessions I did go back and look at what we had done specifically on the Common Rule when we had the opportunity to comment on the advance notice of proposed rulemaking and we did focus on the QI research distinction but there could be sort of other threads where this came up on some other topics like, you know, even maybe when we discussed consent.

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

I think there is something to be said, but that wasn't necessarily listed in the particular testimony that we had so we have to sort of separate what we all know from our experience from what our witnesses said.

But for example, you could imagine confusion in the situation of what is public health authority or what is healthcare oversight. There are a lot of different terms within the regulations that speak to the activity of analysis of data at a large scale without necessarily characterizing it as research and then you have to tease out is it the Common Rule or it not the Common Rule? But I think that's more what we know than what was testified to.

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

Well, that's right, but in terms of our own discussion and recommendations we're not necessarily just limited to what we heard, but you're right that the slides were intended to sort of summarize the testimony. David if there is something in particular that you remember that we did?

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Well, I think the consent issue is the main one.

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

Okay.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

I think it's the different notion of what consent means and the processes whereby it's granted through a human subject review and I mean some of the things that are for example coming up in this recent decision the 23andMe to sell its data to pharmaceutical interests and push back from consumers who didn't understand what they'd consented to and I think that I can't be too much more specific without going back and looking at the notes, but it just struck me that there's more to it than just this notion of what was the purpose you were collecting identical data for, one was allowed, one wasn't allowed.

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

Okay, okay, we'll dive back into that.

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

Hi, Deven, this is Cora.

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

Hi, Cora.

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

I have a scoping question, but did you guys think about including FDA as well as sort of one of the entities in the mix?

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

You know we didn't have anybody in the presentation specifically talk about FDA regulations and that just could have been a gap because, you know, we have folks from the FDA who participate in our calls and, you know, it was not...I don't think we deliberately tried to scope them out so that's a good point.

It could be that we will need to gather some additional information to make sure that we have an understanding of legal regimes that cover, you know, data that is covered by FDA rules. So, you know, for products that are going to undergo regulatory approval or that are subject to regulatory oversight by the FDA. Very good point.

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

This is Michelle, there is a typer if that person could mute their line it would be wonderful. Thank you.

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

Thanks.

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

Unless it's Deven.

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

It was not, sometimes it is but today it was not. Next slide, please. Okay, so here we actually do have, Micky this may be in fact where we have nested the point that you raised earlier because the next bucket of concerns are, you know, what we heard about some of the common tools that are used to protect privacy and confidentiality with respect to data that is either health data or that is being used for health purposes and de-identification is one of them.

And we heard, you know, from a number of presenters that this is a pretty critical tool for protecting privacy, it gets used a lot but there are concerns that persist about what is the re-identification risk of de-identified data including data that has been de-identified in accordance with HIPAA standards but of course, you know, entities that are not covered by HIPAA don't necessarily have to abide by HIPAA standards when they de-identify data and often that term de-identification gets used even when you're not talking about data that have been de-identified in accordance with HIPAA standards.

We have concerns about re-identification risk and this is particularly the case when datasets are combined. There was discussion about the mosaic effect and data that's de-identified using the safe harbor method, one of our presenters in particular raised some issues about the viability of that methodology for protecting against re-identification risks in an increasingly complex health big data environment.

But then again, the safe harbor was intended to be very easy to use in order to encourage people to de-identify data without necessarily having to hire an expert. We don't have any widely applicable prohibition or penalties against re-identifying de-identified data.

When people do use the expert determination we don't have a lot of transparency about the methodologies that are used or objective scrutiny of whether those methods work. And while de-identified data may be useful for a lot of analytic needs it may not be useful for all.

We heard testimony, for example, from Rich Platt about the need to use data that preserves a sufficient amount of identifiers that you can check to see whether in fact a patient has died by using data from the National Death Index.

What other...what might we be missing here in terms of concerns that were raised about de-identification as a privacy protecting mechanism in health big data? Okay, maybe we got a good start on that one. Next slide, please. I'm on slide 11. So, consent was another topic that came up.

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

Hey, Deven, this is Lucia, just going back to the prior slide.

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

Okay.

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

So, if we could just flip back for one second.

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

Okay, can we have the previous slide, please? Thank you.

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

So, I think it's useful to ensure that we capture in here not just that the safe harbor was intended to be easy but it's, also relatively speaking, much more inexpensive than the...it's not just easy but it can be implemented at a low cost which actually facilitates the creation of datasets for analytics.

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

Okay, good point.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

And Deven, this is David, one important tactic that some of the presenters talked about was this notion of data enclaves and I think that's going to turn out to be something pretty important and I'll bet you that this ends up in our recommendations, because it's about the only sane way to think about some of this stuff.

And also, just a little caution that one of the presenters uses the phrase "safe harbor" to mean data enclave so you have to watch out.

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

Okay.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

When you're reading the sentence.

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

Got it, thank you, which is an interesting conflation of what...

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Yeah.

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

Seems like two different concepts.

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

That's the same conflation as "can I have a de-identified limited dataset."

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Yeah, yeah.

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

We'll get that right over to you. Okay, other thoughts on this slide? All right, great, let's move to consent then. Thank you, all, great conversation.

So, again, this is another one where, you know, we had a lot of robust testimony from our presenters, it's a valued tool for protecting privacy and honoring individual autonomy but it's often difficult to obtain, you know, really informed consent up front for future valuable big data uses and re-uses because that requires you to know what they are in advance at the time of collection or be able to go back and re-contact people in order to get them to authorize future uses. It may really not be possible for large scale studies given the volume of individuals you would need to reach.

Opt out was mentioned as a possible option in circumstances in particular where it is hard to reach people for opt ins, but even in some circumstances allowing opt outs may have an impact on the validity of the results.

It puts the burden for protecting privacy on the individual because it relies on them to make judgment calls about what's appropriate and what's not appropriate versus necessarily defaulting to rules.

And it may work best when it's not over utilized. For example, not requiring it for, you know, necessarily uses that reasonable persons would expect that are sort of consistent with norms. So, I want to open up to some comments on this particular issue?

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

So, Deven, this is Lucia, you know, for those of you on the Workgroup who got to attend our four Workgroup call later in December you heard a little bit about electronic consent management so I'm going to try and summarize what might be an additional bullet here, put it out there for the group's consideration.

We kind of have a mismatch, we actually have the...we don't have technical barriers to build tools that collect, adjudicate and persist consent connected to the data that it applies to but we do have barriers, because of all the things we mentioned before, ambiguities, wide variation in the laws makes it really hard to have a computer figure out what the rule is that it's adjudicating and, you know, sort of...does the person who's consent or absence thereof is being persisted understand the implications of it over time and subsequent uses of the data, which are all more sort of policy side questions. And so we sort of have a mismatch between the "how to do it" and the "what are we doing."

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

Or are you suggesting, you know, what might be technologically possible at least with technology that's out there although it may not necessarily be ready.

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

I didn't say it was easy, I said it was possible.

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

Right, right.

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

Yes, we have some technical capabilities that we're maybe not able to take advantage of because we haven't figured out the policy complexities.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

So...

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

That might be something to add to this just, it's just an idea.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

This is David, I just...I think we have some technical capabilities but I'm not sure they're completely robust enough and in particular some of the metadata descriptors necessary to tag the data that might be managed by those technical things don't exist.

The agreement on nomenclatures and granularity of the nomenclatures to describe the types of sensitive data that might be subject to a particular policy aren't very well...aren't very mature and are difficult because of the granularity mismatch amongst users is so profound. One man's sensitive data is another man's visual acuity, you know, and...

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

Right, well, I think you're right but I think if there were more clarity on the policy side the nomenclature would fall into place more easily.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Yeah, it certainly wouldn't hurt. I mean, you can quickly get to the default case of, what's sensitive to an individual is highly individual and it's going to be difficult to sweep it under a broad policy because, you know, there may be certain innocuous facts that are quite revealing in some particular person's settings that make this completely benign in another person and it's going to be very hard to manage that with tags and descriptors. It boils down to what do you think is sensitive in your data, which isn't to say we don't try to get a first pass approximation that addresses most people's concerns but it has its limits.

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

Right.

**W**

Deven?

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

I guess the question David is, is this a concept that's worth including in this bucket relative to big health data as we move forward. I mean, we could have a very long discussion about consent and I know you guys already have.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Yeah.

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

But what do we say about it here because we have these prior reports from PCAST and JASON one which makes some assertions about technology which, you know, technologically aren't far off, and the people that...you know, the Policy Committee and people who will read the report when we're done are aware of that background. So what do we say about that here?

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Well, I mean, that's a great way to ask the question and I wasn't making my comment with an assertion that it ought to be included here, but now that you've asked and I've thought about it a second, I think even in the, you know, in the big data world, let's take the non-healthcare big data world, there are certain things that may jump out at you that your phone knows about you that you had no idea that it knew about you and some people will react to that in thinking "oh, my God that's the creepiest thing, I want to turn that off" and other people think it's the coolest new social network feature they've ever heard of. And it's the same thing but people react to it completely differently.

So, I think what gets difficult is to describe a risk or a threat using standard terms without invoking an individual's own perceptions and that's just the challenge I don't know that it's a...it's just a challenge which makes it hard to do.

It's hard to find a general purpose rule that says "we won't expose your location data to these services" but another person says "that's exactly what I want you to expose." I'm not sure we can turn it into something that would fit on this slide.

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

Yeah, so I'm actually going to suggest that we...when we do the deeper dive on consent that we try to work some bullets that sort of get...have a way of sort of describing not just the sort of policy tension, because, you know, we've got some good descriptors there but to maybe spend a little bit of time exploring the technical landscape because I know we also have...you know, John Wilbanks, who is one of our Workgroup members, who is on the call but is just able to listen he doesn't have phone participation capabilities, he's done a lot of work on this, you know, some of the technical aspects in terms of coming up with some models that he's using too.

So, I think it's going to be worth diving into this a bit but it could be that we just...that we do that when we schedule the sort of deeper dive on this particular topic. Does that make sense?

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

Yes.

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

Okay.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Yes.

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

Great, thank you.

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

So, Deven, this is Micky, two other things, I don't know how you want to do this in the structure of this document, but it seems like, you know, state variation and consent laws if you have a large scale study that crosses states could be an issue and I know we've talked about that in one of the other slides about state variations. So, maybe you don't want to repeat it here, but it specifically applies to consent.

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

Yeah, no, I don't think it's a bad idea necessarily to reiterate it.

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

Okay. And then the other one is, you know, sort of a subset of data provenance which is consent provenance. I mean, how do you, you know, sort of track the consent of a particular set of data as it cross...if it takes multiple hops?

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

And that sounds like you're talking about a technical. Am I right about that? Like how do you persist it or even from a policy matter you need to persist it?

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

I mean, yeah, I mean there are technical...there could be technical solutions to it but I think it's a problem, you know, separate from the question of what the technical solution is to it.

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

Okay.

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

And Deven, this is Cora, I was thinking...

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

And find some...

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

Something along the same lines but not...you know, it's interesting because that comment is an interesting sort of technical solution to what I was thinking of which is the unexpected secondary uses of information which presents its own sort of set of consent issues for which sort of a consent provenance might be one kind of a solution and sort of downstream restrictions are another kind of solution.

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

Oh, yes, well it was no accident that the next slide is dealing also with transparency which is often closely tied to consent. I know that wasn't...Cora that wasn't your sole point, but the sort of unexpected uses...

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

Yes.

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

Is both a transparency issue as well as, you know, well which ones should people have some choices over.

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

Right.

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

Yeah. Anything else before we leave consent and move to transparency? Okay, next slide.

Transparency, here is some of what we heard from our presenters. Consumers, patients lack transparency about actual uses and disclosures of their personal information, what's required, at least for entities covered by HIPAA in the notice of privacy practices is, you know, what do entities have the right to do with data and what patient's rights are with respect to that data, but it's not necessarily what they're actually doing with data.

And we heard some interesting testimony from Rich Platt and there could be others about, you know, we could do...suggesting that we could do more to alert people about the secondary uses of data in learning healthcare systems, which was what his comment was more particular to, but I think you could see where that concept could have value in other contexts.

And privacy policies, which are often driven by need to have legal defensibility but often written to make sure you have that legal defensibility and not always drafted primarily to make sure that consumers understand and they can often be long and hard to read, not always, certainly there are examples of people doing well in this regard, but, you know, we heard some testimony that this is not done as well as might be desirable.

Uses of de-identified data are rarely disclosed in part because the data tends not to be regulated in the ways that identifiable data are. And again, as we noted in a prior slide, we don't have a lot of transparency about, you know, how data are used in terms of the basis for decisions or uses of algorithms, etcetera. There is, in some regard, a bit of a black box quality to this particularly for individuals. What's not right here and what are we missing?

Okay, so next slide, we're on slide 13. I used this slide to cover the last two of the tools that we heard about for protecting privacy and confidentiality that are at least, in terms of tools, within the realm of the fair information practices that includes collection, use and purpose limitations like, you know, not collecting specifying the purpose for which you're collecting data and not collecting more than you need or not using it beyond the original purpose and, you know, questions were raised by a couple of the people who presented to us about whether, you know, putting these limitations on data whether that hinders the ability to gather insight from the data such as in models that we heard about that allow the data to serve as the hypothesis.

And if you, you know, have a policy that limits data collection to what's needed to address a specific question you may not be able to sort of allow the data to essentially surface interesting information.

And data security and we had one presenter that talked about this but this may be one of those areas where, you know, we might seek some additional input from the public because some of the folks that we had reached out to, to specifically address this topic and in particular one of our Workgroup members, David Kotz, who has some expertise in this area, was not able to present to us and unfortunately was not able to be on our call today.

And this is really the end of the sort of section on sort of tools for protecting privacy and, you know, what we heard from our presenters and what we want to make sure that we get out on the table about those tools.

And the next slide deals with harms. So, I think if you've got some issues that you didn't see yet come up that aren't related to harms, you know, now would definitely be the time to surface them.

**Gayle B. Harrell, MA – Florida State Representative – Florida State Legislature**

Deven, this is Gayle, I would just like to comment that I really think we need further conversation on the security.

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

Okay.

**Gayle B. Harrell, MA – Florida State Representative – Florida State Legislature**

That was so abbreviated and I really think that needs to be dealt with in much greater depth.

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

Yes.

**Gayle B. Harrell, MA – Florida State Representative – Florida State Legislature**

And we ought to say that to the Policy Committee and let them know that if it's the will of this Workgroup that this is something we're going to come back to.

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

Yes, yes. Yeah, I think you're right. It's interesting when Stan and I were working with ONC and our staff support from MITRE to pull these slides together and going through the transcripts like, yeah, we did get one person saying something about security and it was really pretty...it was not her area of expertise and we didn't really...we're missing that and we really do need to go back out and gather some input.

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

And Deven, this is Lucia, Gayle raises a really interesting point but it's also instructive to sort of conceptualize it that some of what we heard a lot about was de-identified data which of course is not HIPAA regulated at all.

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

Right.

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

So, the HIPAA security rule doesn't apply which doesn't mean there aren't security concepts or it might be appropriate to list it as a place where de-identified data if not regulated by the HIPAA security rule what does protect it from a security stand-point.

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

Right.

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

Right, as a sort of gap in regulation, but it's actually almost a feature of the gradations of data and the structure and the regulation under HIPAA or not HIPAA.

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

Right, got it, good point.

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

And hey, Deven, this is Linda Sanches.

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

Hi, Linda.

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

Hi, I was just thinking there is such inherent tension between the transparency issues on slide 12 I guess and the limitations listed here on slide 13. You know if you're concerned that the notice doesn't say what they're actually doing and you try to address that then you're not...then you're going to have these limitation issues.

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

Right, right if we're trying to leave open some of this, the uses of data how could we possibly be transparent about them at least at the time of collection is that...

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

Exactly.

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

Yeah.

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

I can...I'm envisioning these federal register notices.

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

Oh, right, because everyone reads those.

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

Exactly.

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

Well, some of us do, but it's because we're nerds.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Well you could at least be transparent about your intent to be open with what you do with the data.

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

Right.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Don't promise that you're going to do nothing but one thing if in fact you intend to do more than one thing. Some people might choose that as an opportunity to not share the data.

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

Right, right. Well, it's definitely...I mean, I think there are a lot of sort of goals that we might see as valuable that could be seen as in potential tension with one another and I do think it is our job to try to unpack that a bit and think about a way to, you know, sort of try to maximize the goals and minimize the down side, you know, you want to be transparent but you have to recognize that there may be some limits to that and what are the limits and what do we still want to see as a goal. I think that's a really valid point.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Deven, this is David, changing the subject a little bit, the one thing that I think...I think this concern is woven through your point and maybe it is sufficiently covered, but I think the thing that jumps out what surprises people about big data is the surprising deductions that can be made when data is joined across these various sources and I don't know if we've got that captured here somewhere.

So, you may authorize a particular...you may share your data for a particular use case over in one corner of the room and share it for a different use case in the other corner of the room and both of those are perfectly comfortable to you but what happens when somebody joins those two together is uncomfortable to you. I think that's the big area of big data at least it's more than a healthcare thing obviously, but if it's healthcare data in one of those corners that's when it gets really surprising.

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

Yeah.

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

I think that's right and maybe Deven, this is Lucia, it's fleshing out the problem of re-identification a little bit.

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

Well it...

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Well, it can be done even with perfectly...I mean, you may share identified data with your, you know, population health company that's managing your companies employees, you may share your identified data with your health club but when they join those two pieces of data together and tell you things about your exercise regimen you may be offended and it's not a de-identification thread it's the fact that the data got crossed across two domains and you didn't intend them to be shared with each other.

**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**

Yeah.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Yeah, I don't know how you write...I don't know how you...I mean, it goes back a little bit to the over under regulation slide, there is nobody to regulate that.

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

Right.

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

Maybe it's just data combination because it is...it relates back to the idea from our first couple of witnesses that there is an argument that all data could be used to evaluate health.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Right or financial, or relevance on a dating network, I mean, you know, when you join data across these boundaries untoward things happen, untoward combinations can be created and the consumer has usually no recompense about that, no recourse to address it or to prevent it, it's not regulated.

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

Right.

**Gayle B. Harrell, MA – Florida State Representative – Florida State Legislature**

Or no understanding of the potential of use of it.

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

Right. Yeah, I think we have to...these are really good points. I think we have to find a way to articulate that because I don't think it's quite as specifically pointed out...

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Yeah.

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

In the ways that we've just talked about and it's important.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Yeah, I mean...

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

...

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

It's emergent harm that can occur...

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

Yeah.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

When data that is...you're perfectly comfortable with it in isolation but in combination it creates an emergent potential for harm.

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

And this is Kitt Winter; I just wanted to mention one thing that seems to be missing is the medical ID theft.

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

Okay, I...let's...we're going to harms next.

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

Oh, I'm sorry, I thought we were...

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

And, you know, we don't specifically mention it there either.

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

I thought that we were in the harms.

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

Oh, we're getting there but, yes, some of these discussions have...some of the most recent discussions, you know, touch on harm issues, harm or surprise but we don't have identity theft on there. So, we will make sure that we do because that's a good point.

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

This is Gil Kuperman.

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

Hi, Gil.

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

Hi, you know, just back to that issue that David McCallie was mentioning a moment ago that, you know, I was thinking about the same thing or something similar that it's...most of the regulations these days deal with data from health providers rather than information about health status and I wonder if that's maybe a comment about regulation that, you know, might be worth making. I mean, it's very broad and overarching and it might be too big, but in some ways it's...I think it kind of gets at that. I don't know if that's helpful.

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

We did have testimony about the fact that the regulations we have today are business sector specific, that's how I would characterize it, I know that's probably not the words of the witnesses, but that's really what you're talking about, it's not about the content itself it's about what part of the overall American universe does it get collected in.

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

Yeah, I think that gets at it. I mean, the one that kind of sticks in my mind is, you know, when Uber knows that you're going to the cancer center, you know, what controls are put on their use of that data and, you know, so I don't know if that's exactly what David was getting at but I think it's the same kind of theme. I don't know if it's worth trying to make that point in the regulation section.

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

I think it's...we definitely heard about...you know, I think it is a combination of, you know, data that is used or usable for health and how that could be quite distinct from health data, but has its own sensitivities and what...and that's a great concern whether it's because it gets combined with data from, you know, from another area of life and used in ways that people don't want which was David's point I think or whether it's just that somebody can have access to it and, you know, potentially use it at all even without combining it with another type of data.

So, you know, whether its Uber knowing exactly where you're going to, you know, your grocery store bill suddenly, you know, showing up, you know, somewhere where people are evaluating your eating habits in terms of making drawing conclusions about your life expectancy and health data even though you might not be being treated by a healthcare provider for anything related to bad nutrition. I mean, you know, you could come up with lots of different examples here. So, I think, we need to flesh that out here too.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Yeah, this is David; those are exactly what I was talking about. I mean, you know, there are domains where we wouldn't think twice about clear inappropriateness of reuse of the data so for example, if I give my credit card number to Amazon to purchase something I'm comfortable doing that but I'm certainly not authorizing them to use that credit card number to purchase something else.

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

Right.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

And if they tried to do so I would sue them. But in this more nebulous realm of all this personal data that we are perfectly happy to share with a service provider in exchange for a particular service we have little say or visibility as to what happens when they take that data and do completely different things with it than the service itself that we purchase or that we engaged with.

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

Right.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

So, there are some things that we clearly wouldn't think twice about that's wrong and in this new space I don't think people have thought it through yet, how much of it is acceptable and how much of it should be either more carefully regulated or the harms that can come from it more clearly addressable.

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

Yes.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

And that's the whole PCAST, that was their conclusion, is you can't stop it so you'd better focus on the harms that can come from it.

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

Right.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

But anyway that's jumping ahead.

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

Well, that's okay, let's...unless someone has an objection let's go ahead and go to that next slide which is slide 14 on harms where we did have a number of presenters that urged us to consider protections that would either prevent or limit harms to individuals caused by collection, use and disclosure of big data health.

And we pressed a number of our presenters on, you know, sort of what sorts of harms are there that we need to take into consideration and what would potentially be ways that we could limit or redress them and I think we got a fair amount of testimony on what some of the harms would be maybe a little less testimony on how you would address them, but certainly when we dive into this issue in more detail we'll go back and go through the testimony and see if we missed anything but also maybe consider whether we have some more folks that we need to talk to.

And some of the harms that we did hear about were discrimination otherwise referred to as data redlining which is a term that Lucia used and I think it's a very good encapsulation of what we might mean by, you know, discrimination using data or a form of discrimination using data.

We don't have medical identity theft on this list and we need it or identity theft generally but since we are dealing with health data the medical identity theft certainly is relevant.

Embarrassment or harms to dignity from the exposure of information that people intended to keep private. The harms can be either to individuals or to groups when data are used to make decisions that are applied to groups that have a discriminatory or harmful impact on them.

And then a harm to trust in terms of people's willingness to put their data into an ecosystem that might provide them with some advantages but where they just are reluctant to do so because they don't have the kinds of assurances or protections that they might need in order to do that and whether that's, you know, not wanting to seek medical treatment for certain conditions or just not wanting to, you know, pursue options in the consumer space such as Apps or social networking sites that might otherwise be beneficial because of concerns about data use.

What are we...other than medical identity theft which Kitt has identified which we need to include in here, what are we missing in terms of this harm discussion?

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Deven, it's David, do you intend to include financial harm under the data redlining thing or is that a separate category, I mean loss of employment, inability to gain employment, loss of insurability?

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

Yeah, you know, we should flesh that out more. That was intended to be subsumed in there but it's...we need to spell that out I think.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Then the only other thing I would add is, in your individuals or groups, I think in the genomics world that we live in it can also be harm to your family.

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

Yes, even family history data.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Well exactly, I mean, you could disclose something that has a deleterious effect on your children unbeknownst to them for years to come but it will be out there someplace.

Also, so you include communities when you say “groups?” I’m thinking of the Robert Wood Johnson Data for Health discussions that you and I are part of.

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

I think it’s worth fleshing that out.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Okay.

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

Because groups could be...

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Pretty big.

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

Subpopulations but communities is another, you know, there are different dimensions to that which we should flesh out. Okay, that’s great, this feedback is tremendous. So, we had...next slide, please. We tee’d up...okay, I think we had...we got some good feedback.

If anybody thinks of something off line that doesn’t occur to them on this call, you know, feel free to send us an e-mail, because again we’ll be diving into these topics in more detail so there will be an opportunity to flesh them out but it’s good to get some feedback from all of you about our initial cut on where these themes are.

And so we are going to dive into de-identification first, next slide, so we’re on slide 16. And so we earlier identified some, you know, potential issues that arise with respect to de-identification and some of them are articulated, re-articulated here but also there are some new topics on this slide.

So, you know, we’ve got the issue of, you know, how do you generate de-identified data, we’ve got the safe harbor as the simple and as Lucia pointed out the less costly option for de-identifying data but we heard testimony that it’s more vulnerable to re-identification risks and yet we have little transparency in the expert determination method even though we were urged, by at least one presenter, to rely on this more heavily because if it’s done well it is perceived to be more protective.

We don’t have a prohibition on re-identification. We have issues of utility. If you’re relying on de-identified data it’s sometimes not enough data to address the particular question that you need to address.

You know what are the risks of re-identification? We, you know, had some testimony from one of our presenters who is an expert and written a number of books on this topic that the threat is not, of re-identification, is not necessarily as acute as has been presented in some reports, you know, but even upon questioning he, you know, shared that certain methods of de-identification, again, safe harbor, are more vulnerable that combining datasets makes re-identification potentially more possible and that we, you know, certainly the perception is out there pretty widely that this is...that re-identification is certainly not the be all and end all of protection there.

And what sorts of provisions might we put into place in order to shore up de-identification as a privacy tool not necessarily the only one but one of them. You know defining standards for the expert determination for example and ensuring methods are published or scrutinized might be another idea to consider.

Should we have experts certified or required to meet certain professional standards? Can we encourage people to use the expert method more often by packaging that expertise in ways that allow expert derived methodologies to be deployed through automation for example?

And so on the next slide, which is slide 17, we start to sketch out what some possible solutions might be here and we can and should consider to continue to talk about sort of making sure we've sort of fleshed out fully what the issues are with de-identification and if need be identified areas where we need to do a little bit more digging.

But some of the topics that we, you know, have sort of tee'd up for your consideration and, you know, I see we're sort of ending our call, we're close to the end of the time for our call here today so we'll be picking this up on our next call, but, you know, some of the ideas and we already started to articulate them on the previous slide include, you know, setting de-identification standards for all personal data, you know, HIPAA has a standard that's required of covered entities and many people not regulated by HIPAA use or rely on that standard but absent HIPAA there are no standards out there, maybe there ought to be standards for de-identification of health data that apply more broadly.

Do we need to provide more incentives for using de-identified data? We define standards for expert determination and ensure that there is some way to publish or if not publish at least have objective scrutiny of those methods, certification again was mentioned, packaging the expertise, prohibiting re-identification, requiring re-assessment of re-identification risks and any time when datasets are combined so that de-identification is not, you know, if done once isn't considered to be evergreen that there is a subsequent evaluation if new data are introduced to that dataset or the dataset is combined with another dataset.

Do we have some minimal security requirements that would apply even in the case of de-identified data?

And is there the potential for not requiring such a stringent standard for de-identification for certain research purposes where there are additional data points that are needed to address the question but there still is an effort to remove identifiers that increase risks and one could put the limited dataset in this category but I know, you know, for some this is about creating sort of a sliding scale of protections that, you know, that where you have other contextual...whether you have other protections for the data you don't necessarily need to rely so much on the de-identification of the data to enhance it.

So, for example, the data enclave, I know that when Khaled had testified about this he said, well, you know if you're making the data available in a data enclave so people can't download it and can only analyze it within that enclave, you know, that's a set of protections that might allow you to persist more identifiers than the dataset without needing to de-identify it to the point that you would need to if you were making it publically available.

So, that's just intended to get us started not intended to be the be all and end all, but what we're hoping to do, again, is both to have a robust conversation about this issue but really begin to sort of think about, well, how would we address some of the concerns that were surfaced in the hearings.

So, I'm looking at the clock and seeing that it's 21 minutes after the hour and we're close to the time when we need to go to public comment so does anybody have anything that they...I think I can entertain a couple of minutes of conversation among Workgroup members just at the close of this Workgroup call and then we'll begin with this anew and fresh on our next call. But, does anybody have anything they want to share now before we move to public comment.

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

Hi, Deven, this is Linda Sanches.

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

Hi, go ahead Linda.

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

I'm just wondering if when this discussion continues and you're crafting the recommendations some of these would require some sort of new statutory authority...

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

Yeah, yes.

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

While others would not and so it might be helpful if we're thinking about that that we're clear about what we're asking for.

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

Yeah, no, absolutely that's a really good point. We could characterize the solutions in that way and we'd love to have some help.

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

Yes, always available.

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

Thank you.

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

Hi, this is Stephania Griffin over at VA.

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

Hi, Stephania.

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

I agree with the past comment, but I also would ask, at least in HIPAA, the de-identification standard is the same whether you're trying to use the data internally for a purpose or whether you're trying to disclose it externally to another entity to use for some purpose whether it's research or something else and that's one of our biggest struggles right now is internal versus external and so as you look to maybe strengthen the standards and you look to put some more framework around it I do want...I think that should be part of the conversation is how does that impact really internal use of de-identified data versus what I think most of us think de-identification of data is for is kind of this external sharing and disclosure. But there is a lot of internal use that goes on as well.

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

Okay, that's a good point Stephania, thank you.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

And Deven, this is David.

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

Go ahead David.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Just you mentioned data enclaves but I don't see them on your possible solutions list.

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

Yeah.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

Unless I'm misreading it.

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

Good point.

**David McCallie, Jr., MD – Senior Vice President, Medical Informatics – Cerner Corporation**

I think that that's such an important concept that we ought to bullet it.

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

Okay, got it, good point.

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

Deven?

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

Yes?

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

Hi, Gil Kuperman here again, you know, it seems that the concerns really split out into two categories one is making de-identification more straightforward and easier so that it can advance the goals of the learning health system.

There is another set of concerns that relates to, you know, privacy risks related to de-identification and, you know, maybe the approach is to tackling each of those would be different and, you know, then maybe, you know, splitting those out might be helpful, just a thought.

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

Okay, no that's a good suggestion. It's both about making it easy to use but also about, you know, how do we deal with the privacy concerns that people have with respect to it.

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

Yes.

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

Okay, well, it's 3:25 so got to appreciate even the input that we've been able to get in the short time that we had left on the call. We'll pick this right back up focusing on this de-identification topic on our next Workgroup call. And so anybody who didn't get a chance to chime in and you want to get a thought off so you don't forget it in two weeks please just go ahead and send us an e-mail. Michelle, we're ready for public comment.

**Public Comment**

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

Operator can you please open the lines?

**Lonnie Moore – Meetings Coordinator – 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.

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

We have no public comment at this time.

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

Okay, great, thanks a lot Michelle, I wish everyone a good rest of your day and look forward to picking this right back up in a couple of weeks.

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

Thanks, everyone.

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

Thanks, Deven.

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

Thank you.

**Gayle B. Harrell, MA – Florida State Representative – Florida State Legislature**

Bye.