



**HIT Policy Committee
Privacy & Security Workgroup
Big Data Public Hearing
Final Transcript
December 5, 2014**

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 Privacy & Security Workgroup...I'm sorry, the Health IT Policy Committee's Privacy & 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?

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

Here.

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

Hi, Stan. 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?

Donna R. Cryer, JD – Principal – CryerHealth, LLC

Here.

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

Hi, Donna.

Donna R. Cryer, JD – Principal – CryerHealth, LLC

Hi.

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

Gayle Harrell? I believe Gayle is on. Gil Kuperman? Gwynne Jenkins? Helen Canton-Peters? I'm sorry.

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

Thank you, from ONC. 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?

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

Here.

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

Hi, Kristen. Linda Kloss?

Linda Kloss, RHIA, CAE, FAHIMA – President – Kloss Strategic Advisors, Ltd.

Here.

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

Hi, Linda. Linda Sanches?

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

Here.

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

Hi, Linda. Manuj Lal? Mark Sugrue? Micky Tripathi? Stephania Griffen?

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

I'm here.

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

Hi Stephania. And Taha Kass-Hout?

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

I'm here, thank you.

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

Hello. And from ONC, we heard we have Helen Canton-Peters. Do we have Lucia Savage?

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

Present.

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

Hi, Lucia. And Kathryn Marchesini?

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

Here.

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

Hi, Kathryn. Okay, and with that I'll turn it...

Gayle Harrell, MA – Florida State Representative – Florida State Legislature

And Gayle Harrell is here, too.

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

...back to you Deven and Stan.

Patricia Flatley Brennan, RN, PhD, FAAN – Moehlman Bascom Professor, College of Engineering – University of Wisconsin – Madison

This is Patty Brennan; I just want to let you know I'm in the room now.

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

Oh great, thank you.

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

And hi, it's Micky Tripathi, I'm here, too.

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

Oh, great.

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

Hi, Micky.

Gayle Harrell, MA – Florida State Representative – Florida State Legislature

Gayle Harrell, also.

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

Hi, Gayle. Okay, Deven and Stan, sorry.

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

No worries, Michelle. Thank you very much. I want to thank everyone for making time for this first session of our public hearing on Health Big Data, opportunities, learning health system, concerns, what's current law? How do we address it? This is our first session today; we have another session scheduled for Monday. These were not meetings that were originally meetings of our Privacy & Security Workgroup, so for all folks who had to make some schedule adjustments to be able to be with us today, both on the workgroup, of course our panelists, but also members of the public; we very much appreciate it.

I know that I am really looking forward to this day, as well as to Monday. I think there's a lot that we're going to learn from the panelists that we've amassed and it's very exciting to be diving into this in detail.

Just to give you a little bit of an overview of how the day is going to go, we have three panels that will be...and on each panel we have presenters who will each take 5 minutes to share their thoughts with us. But then we have 50 minutes on each panel for discussion, for workgroup members to ask questions of the panelists or panelists to interact with one another and for us to stimulate even more dialogue on the issues that come up.

The way that we handle the Q&A is, on the top of your screen if you are online, you'll see a little icon with a person who has their hand raised. As a workgroup member and this is for workgroup members only, you can put yourself in the queue by clicking on that icon and raising your hand. And what that will do is queue you up and then whoever is moderating the panel, either Stan or myself, will call on you in the order in which your hand is raised. We do like dialogue as part of these discussions so there are certainly occasions where your question may be lower on the queue but someone else asked a question that's related to yours and staying on that topic it makes sense for you to chime in with yours. And we certainly have allowed this to go with the flow, for lack of a better term. But inevitably our hope is to allow everyone that has a question on the workgroup to be able to ask one.

Panelists do not have to raise your hand, you are on the panel you interject when you want to make a comment or want to provide some follow-up food for thought on something that one of your panel colleagues has mentioned or you have a question that you want to ask them. So, you don't have to use the raise hand function to do that while you're on the panel, that is part of the gift that we give you for being willing to come and do this for us. Your comments have some priorities for us, as panelists. But otherwise, workgroup member's need to raise their hand.

And then of course, at the end of our day, as always, we will open up the lines for the members of the public who are listening in to provide some comments. And we'll do that also on Monday, as we do with all of our public meetings.

So, I also...on that raise hand function, I suspect that we may have a few working group members that -- are not...are just following the audio on the teleconference and were not able to be online. If that's the case, just make note if you have a question and we will...make note verbally if you have a question and the moderator, either Stan or I, will put you in the queue. Does anybody have any questions about that?

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

Deven, I have one observation. This is David.

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

Sure.

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

Just from previous experiences on both sides of the table, when we ask questions of the panelists, they don't all need to feel compelled to answer, the questions can be directed or answer if you think you have something to add, but don't feel compelled to.

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

Yeah.

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

That's been a point of confusion in the past.

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

So thank you, David. Absolutely, if it's a question that you don't want to answer or they don't really have any input on, you are perfectly free to remain silent or just say, I don't know. Any other thoughts?

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

Yeah Deven, this is Lucia. I think that really deserves driving home. We don't expect everyone to know everything, we're here to find out what we do know so that we can find out what we need to find out.

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

Yeah, yeah, good point. All right, so with that, before we start the first panel, we wanted to do a few introductory slides. These will be familiar to the workgroup members because we've gone over them before, but for the benefit of the panelists and the public on the phone, I think it's worth talking about why we're doing this in the first place. What we're sort of trying to drive at, in terms of this opportunity for us to hear from panelists and then we'll, as a workgroup, go into several weeks, if not months, of deliberations on what we heard and so I think it's a legitimate question to say, well what are we really aiming at here? Why are we doing this?

And so, I think, so we just have a few slides here, just as introductory slides, so that we have a...we level set the understanding for all on the phone about what we're really trying to achieve here. So, It really starts with the report on big data that came out of the Executive Office of the President in May of 2014. And that was a report on big data broadly, but it did have a number of relevant and very specific comments to make on the issue of health big data, and here's one of them, specific recommendation from the report. The government should lead a consultative process to assess how HIPAA and other relevant federal laws and regulations can best accommodate the advances in medical science and cost reduction in healthcare delivery that are enabled by the big data.

Similarly, some other pieces of the report noted the need to build a learning health system. Also, that the privacy frameworks that currently cover information used in health may not be well suited to address developments in big data or facilitate the research that drives them. There is a need for advanced analytic models in the big data context. But, that big quote that's on the right-hand part of your slide, I think really hammers it home which is, that the complexity of complying with numerous laws when data is combined from various sources raises the potential need to carve out special data use authorities for the healthcare industry if it is to realize the potential health gains and cost reductions that would come from big data analytics. So, some real questions raised about whether the frameworks that we rely on today to govern uses of health data are going to be sufficient to address this new environment.

And then following on the heels of that Big Data Report is an announcement that came out of the White House on the 3rd anniversary of the Open Government Partnership that announced some new open government commitments. And I'm sort of skipping down to the end of this slide, which really gives us some sort of marching orders for what we're trying to accomplish here, which is, to ensure that, you know, acknowledging again that big data introduces some new opportunities, that's partly what we're going to explore here today and Monday, but to ensure that individual privacy is protected while capitalizing on these new technologies and data. The administration, led by HHS, will consult with stakeholders...to assess how Federal laws and regulations can best accommodate big data analyses that promise to advance medical science and reduce healthcare cost and develop recommendations for ways to promote and facilitate research through access to data, while safeguarding patient privacy and autonomy.

So, that is our challenge and the reason why we're having these listening sessions is to have a better understanding of what the opportunities are out there as well as the challenges and concerns and whether we have sort of the right policy frameworks in place in order to maximize what is good about what health data presents for us, while addressing the concerns that are raised. And so we're having these hearings and then we will we engage in several weeks subsequent to the hearings of deliberative process to think through what we've learned from the hearings. These are all part of our public calls and to think through what recommendations we would have for how to move this forward. So that's just a level set on why we're doing this. Stan, to have anything to add?

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

No Deven, you've covered it really well.

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

Okay, so great. Again, we're...our job here is to learn, I think Lucia's point was well taken that we want to understand if there are even gaps in knowledge that we need to be exploring as part of this process. We want to know where those gaps are, engage in robust discussion with our stakeholder group, that is our working group, so that we can provide a set of recommendations, it won't be the only set of recommendations that will be provided on this topic, but it will be what I...hopefully, a very thoughtful set at the end of the day. Questions or comments from any workgroup members before we started into our first panel?

All right. Well, that is terrific. We're ready to go with our first panel and our first set of speakers. And so our first speaker is Steve Downs, who is the Chief Technology and Information Officer for the Robert Wood Johnson Foundation. Very pleased to have Steve with us today, I hope he's on. Steve, are you on?

Stephen J. Downs, SM – Chief Technology & Information Officer – The Robert Wood Johnson Foundation

Yes, I am Deven.

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

Oh, terrific. Well great, thank you so much. If you're ready, you can take it away.

Stephen J. Downs, SM – Chief Technology & Information Officer – Robert Wood Johnson Foundation

All right. Thanks Deven, thanks to all of you for the opportunity to present today. Robert Wood

Johnson Foundation has a vision of building a culture of health where everyone has the opportunity to make healthy choices every day, where our healthcare system consistently delivers high-value care and where people work across sectors to improve the health of communities. In short, it's a vision where health is a fundamental American value.

Achieving a culture of health involves recognizing that much of what drives health occurs outside of the formal healthcare system. While medical care is undoubtedly important, health happens where people live, work, learn and play; in the communities where they walk and buy their food, in their workplaces and in the schools they attend. Health plays out in our daily routines, what we eat for breakfast, how we get to work, whether we have opportunities for physical activity, the environmental exposures we receive and the stress upon our mind and bodies. Research has shown that these day-to-day experiences and health behaviors are strongly affected by a set of nonmedical factors; factors such as income, education, housing and access to transportation. Collectively these are known as the social determinants of health.

I see great opportunity for benefit in the utilization of data associated with the social determinants of health. As payment models evolve and as healthcare providers grow more accountable for the health outcomes of their patients, they will need to pay increasing heed to the role that social determinants play in those outcomes. One can imagine healthcare systems leveraging data on housing stock, on community walkability, safety and violence, availability of early childhood services, food accessibilities, transportation infrastructure and more, to understand the barriers faced by individual patients and by their population as a whole.

For example, RWJF young leader Ruben Amarasingham at Parkland Health and Hospital System in Dallas has successfully been using social determinants data to develop predictive algorithms to understand which heart failure patients are at risk for readmission and then take action. There is also a potential benefit in using personally generated health data. Increasing numbers of people are using smartphone Apps and wearable sensors to generate data about an ever widening array of health-related behaviors and experiences.

Apps and wearables track diet, steps, workout, sleep, mood, pain, menstrual cycles and heart rate. Recent products also include hydration, stress and breathing rates and patterns. Still others are able to infer health experiences by analyzing data such as location, movement and social activity, not typically considered health data. These Apps and wearables are providing a new window onto people's day-to-day health.

Three characteristics of personally generated data, the breadth of variables that can now be captured, the near continuous nature of its collection and the sheer numbers of people generating the data, make it extremely interesting for research. And we're seeing some early examples emerge. RunKeeper has used data it collects on peoples' workouts to post information on the frequency, average pace and average distance people run in different US states. Massive Health, a company now owned by Java used data on 500,000 meals from its eatery App which had people photograph and rate the healthiness of their meals to profile how America eats. They generated interesting possible insights including the suggestion that people who eat breakfast eat healthier all day long than those who don't.

These are early and very modest examples of how these data might be used. There is much work to be done before the promise of using these data for research can be fully realized, so we launched the Health Data Exploration Project to look into this topic and found that key issues included privacy, informed consent, access to the data and data quality. The fact that adoption of smartphone Apps and especially wearable sensors is skewed demographically poses methodological challenges as well. We're now supporting a network of researchers, data scientists from companies that gather data and others to work on these issues.

Data on people's everyday patterns can also be used to help public health and other government agencies to understand community needs, make interventions and monitor the responses to those interventions. For example, the city of Louisville is working with Propeller Health with makes the GPS connected asthma inhaler. Together they're mapping hotspots of inhaler use in an effort to understand the environmental and neighborhood drivers of asthma in their community. The Oregon Department of Transportation is working with Strava, whose App helps cyclists track their rides to analyze when and where people ride bicycles so they can see where bike lanes are needed or where current traffic patterns might pose safety threats. Again there are issues like representativeness, access to the data, privacy and user consent associated with using this sort of data featured in these examples for public health purposes. Nevertheless, the example suggests that there might be promise in applying personally generated health data to certain public health questions.

We are very much at the dawn of these new possibilities. We've seen glimpses of exciting potential benefits, but there are cautions to be heard and challenges to be overcome. In every technology innovation and adoption cycle, many of the imagined benefits will not pan out and many of the challenges will turn out to be just transitional. Given the early stage we're in, full of possibility and also potential pitfalls, it is important for us to allow experimentation for the technology and the methods to get better. And most importantly, to allow our institutions to catch up so that they can learn how best to take advantage of these opportunities and realize the potential benefits most fully. Thank you very much.

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

Great, thank you, Steve. That was just about...I could sense you were wrapping up, it was maybe about 30 seconds over. But having said that, it was really great testimony and it sounded like it was going to wrap up. So if all the panelists, and I'm only raising that by way of example for others, that was just perfect in terms of the length.

Stephen J. Downs, SM – Chief Technology & Information Officer – Robert Wood Johnson Foundation

Great, thank you.

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

So that's...thank you very much. Don't go anywhere because we'll be having questions for you. But in the meantime, we're going to turn to our next panelist, Rich Platt, who is the Professor and Chair of the Harvard Pilgrim Healthcare Institute Department of Population Medicine. So Rich, I know you were on earlier.

Richard Platt, MD, MSc – Professor & Chair, Department of Population Medicine – Harvard Medical School; Executive Director – Harvard Pilgrim Health Care Institute

Sure, I'm happy to do that.

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

Okay, perfect. I can't remember did you have slides?

Richard Platt, MD, MSc – Professor & Chair, Department of Population Medicine – Harvard Medical School; Executive Director – Harvard Pilgrim Health Care Institute

I do have slides.

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

Okay, so just holler. The folks from Altarum who help us pull these meetings together will advance your slides, all you need to do is just indicate when you want us to turn.

Richard Platt, MD, MSc – Professor & Chair, Department of Population Medicine – Harvard Medical School; Executive Director – Harvard Pilgrim Health Care Institute

Okay, turn. So as a foundational comment, I'll say that we live in an environment in which despite all the progress that's been made in learning how to provide the best care to the right people at the right time; we still don't know the right answer for a very large majority of the questions that are of interest. And this is just one examples of a review of clinical practice guidelines showing that most of the guidelines for cardiology are based on less than the highest quality evidence. Next. And that's the reason that we talk about a learning healthcare system, one that embeds learning right into the fabric of the delivery of care. And in order to do that, we need to be able to take advantage of the information that is increasingly available in electronic form. Next, please.

So, these are the kinds of things that electronic health records and billing data are really irreplaceable for. First, by themselves or in conjunction with other kinds of data, the kind was just discussed during the last presentation, it's possible to address many very important clinical and public health questions, and I've listed five big categories on this slide. Secondly, there is another large domain in which observational data, that is these data alone, don't provide the full answer and in which we need to do clinical trials, but these kinds of data really can enable a much more efficient and productive clinical trial capability, as well. Next, please.

The things that I use as sort of fixed landmarks in thinking about how can we best use health data are first of all, sometimes you need to use fully identified data. For instance, if you have to match the information in electronic health data to an external source like the National Death Index. Secondly, it is not possible to obtain individual consent for all uses of individual's data. The third is that it is impossible to notify every individual personally about all uses of their data and it really isn't going to be possible to provide universal opt-out provisions, because they can make the answers unreliable. Next, please.

The criteria that personally I think would be appropriate ones to require for using electronic health data are to say that as a general principle, the minimum necessary amount of identifiable data should be used to answer a question. There should be good processes for approval and oversight. The uses of data should be stated publicly and the number of individuals who have access to identifiable data should be minimized. Next, please.

I'd like to illustrate with a couple of examples of work we're doing with the FDA as part of the Mini-Sentinel Project. Next, please. The first is an exa...and the way that the Sentinel minimizes the use of identifiable data is by using a distributed data system in which each of these data partners maintains both physical and operational control over its data. Next, please. The system is a query health reference system because of the way it minimizes the use of identif...the transfer of identifiable data. Next, please.

Data is transformed into a standard format in each location, that means it's possible to send a computer program to each of the sites so they can execute the program and then return the results, which usually don't have identifiable data. Next, please. There's a large data set that has data on over 100 million people, hundreds of millions of person-years; that's why I say it's not possible to notify each individual about the every use of data. Next, please.

Here is an example of the use of data from a million people who were new users of blood pressure control medicines, looking at the occurrence of a fairly unusual intestinal complication. I circled olmesartan, because that's what FDA was interested in and you can see, there's nothing interesting going on here, but on the next slide, you can see that if you restrict the analysis to people who have taken the drug for at least two years, there's an excess among olmesartan users. That's a study that didn't use any identifiable data. Next, please.

Since I'm over time, I'm going to skip over this example. Next, please. Next, please. I just want to show that we used data from over 1.3 million infants, but had to review 300 charts to determine who had the complication of interest. So that was fully identifiable data that had to be used. Next, please. And that resulted in a change in the labeling of the drug...of the vaccine. Next.

So, let me conclude by saying it's possible to greatly eliminate or reduce the need to transfer personally identifiable data by using systems like this, but sometimes, it's necessary to use identifiable data. When you use identifiable information, it should be stored in highly protected locations like data enclaves. And I'll just leave the last slide for the public record, but don't need to talk about it. Thank you.

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

Great. Thank you very much, Rich. Very, very helpful. So the third person on our panel is Patti Brennan, who is at...oh, I'm going to butcher this name Patti, the Moehlman...

**Patricia Flatley Brennan, RN, PhD, FAAN – Moehlman Bascom Professor, College of Engineering-
University of Wisconsin – Madison**

Bascom...

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

...Bascom Professor at the University of Wisconsin College of Engineering.

**Patricia Flatley Brennan, RN, PhD, FAAN – Moehlman Bascom Professor, College of Engineering –
University of Wisconsin – Madison**

Thank you very much, Deven and to the panel for inviting comments in this. Could we go back to the first slide, please?

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

I'm sorry, that was my bad. Altarum, you can handle this for me.

Patricia Flatley Brennan, RN, PhD, FAAN – Project Health Design National Program Director – University of Wisconsin – Madison

I want to pause here for a minute because my topic is to talk about incorporating patient data and learning from it and so we're going to talk about tiny data, medium-size data and massive-sized data. But I want you to take a look at this slide because I want you to think about that redline is reflecting a year in the life of an individual who has an MI at the beginning of the year, goes through a series of care processes through the year and ends up actually a little better at the end of the year.

But I want you to focus for a moment on the skinny little lines which represent the healthcare delivery system as we know it today. And often when we hear about the learning health system, we're talking about those skinny little lines and not the space between the lines or the white spaces. We like to refer to those as the care between the care. And as we think of a learning health system of the future, we need to think about not only the skinny little lines, but the spaces between them, so that our health data flows into and across and between them. Next slide, please.

From our work with Project Health Design, we came to a very clear understanding that professionals are experts in clinical care, people our experts in everyday living and both of these generate a type of health data that requires attention, protection and transmission. Next slide, please.

In particular with respect to the patient participation, Project Health Design taught us a lot about patient generated data and we hear the term patient generated data to mean a number of different things. But essentially this is data that originates in the individual, wherever they are in the world. And I'd like you to think about it as two different types of data, patient sourced data and patient defined data. Patient sourced data refers to things like a self-monitored blood pressure or glucose, where only the person can give you that, even a self-report on a palm scale or a PQ9.

Patient defined data are, on the other hand, the subtle cue sensations that people understand and pay attention to that activate them towards health; we call those activities of daily living. We've done a lot better, frankly, in characterizing the informatics, information flows and protections around patient sourced data, a lot less well around patient defined data and yet what patients pay attention to and listen to is what we really have to activate so we can be careful and attend to the care between the care. The next slide, please.

In the management of chronic diseases, we see also a huge amount of clinically generated data and there has been a great deal of progress in trying to move clinically generated data into the hands of patients; the Blue Button Initiative being but one of these. The challenges we see for researchers and for clinicians of the future is integrating patient generated data and clinically generated data into a total picture of an individual. This is also frankly a challenge not only for clinicians, but also for people who manage population health, public health and people who manage clinical research enterprises. I'm going to leave this now and go on to the next slide though, because I want to talk specifically about what does a citizen need?

What does a patient need because remember, health fits in and around the living space of an individual. And the healthcare system has a good set of tools to protect data, to generate data, to store data, but the health system of a person is more than the healthcare system. Information must flow two ways, back and forth in the individual's life and to those outside of the life, those outside their everyday living into the care delivery system. So our industrial view in the center represents a care delivery system and all the other spaces around represent the everyday lives of people. Next slide, please.

I'd like to talk a little bit about, to address some of the policies that are needed. Some of the policies that are needed to ensure that the data for health be available to the people are outside of the purview of the healthcare delivery system and they include robust and secure network connections. We need to find partnerships with other parts of the industry to address the technical infrastructure. Next slide, please.

However, there are things that are within the policies of healthcare and healthcare delivery and they include access control and privacy mechanisms and interoperability. The access control and privacy mechanisms have to be all along the data continuum from the individual user in the home or sending the data to a clinician, to the clinical care facility that may be aggregating to a large researcher that may be taking broad bases of data. So we need access control and privacy mechanisms that are at the level of data use, not just at the level of data generation. Next slide, please.

And the interoperability models have to actually move in and out of professional care delivery systems, professional data management systems, in and out of the back pockets where people are storing their cell phones. Now as we think about this, I want to just make two points here about big data. One is that there needs to be understanding that local analysis as well as central analysis of the data will both be important. That is, how we analyze the number of asthma puffs a patient takes off their inhaler at the moment may be important for that person, how we aggregate that for a community brings a different level of challenge. And secondarily, the storage of this rampant and rapidly increasing data types is really not well thought through. Next slide, please.

I want to return some comments that Steve made to say that we now see a middle ground of data occurring between patient defined and patient generated and that is this current interest in social and behavioral domains...determinants of health. And the final slide, please. And to just call your attention to work that was recently released by the Institute of Medicine on capturing the social and behavioral domains in the electronic health record. This report that came out last month does address some of the considerations related to care, privacy and data storage. And thank you very much for your time and your patience with me.

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

Oh Patti, that was terrific. Everyone really managed to do a tremendous job with that ridiculously short amount of time that we gave you and we really appreciate it. There is also, just for folks who maybe don't know this already, we do...all of our public hearings are transcribed. So there will be an opportunity to go back and review people's testimony as well as the answers to the questions. And we don't time you on your answers to your questions, by the way, so everyone can take a deep breath, now.

But this is really fabulous. So I'm going to ask for workgroup members who have questions to go ahead and use their little hand raise function and begin queuing up. But I'm going to get us started with a question that was raised in your presentation, Steve, but I certainly would invite the other panelists to address it. You talked about how, you called it an issue where we don't necessarily have representative data from some of these sources because not all communities are sort of robustly using Fitbit and Jawbone and some of these other types of technologies that are out there today. And I want to give you a chance to sort of expand on whether...what are the issues with respect to who's using these types of tools versus where we want to make sure that the benefits of the learning heal...a larger learning health community accrue to?

Stephen J. Downs, SM – Chief Technology & Information Officer – Robert Wood Johnson Foundation

Yeah, thanks for asking that. I think there is a bit of a stereotype that says the people that are using the Apps and wearables are sort of the tech savvy, affluent, worried well. I think the folks who sell those products now would tell you they've moved well beyond that, but it's still skewed. It's changing. It's dynamic and what it does is it raises issues, particularly for let's say the public health applications. And if you talk with and say folks at RunKeeper, they would say if you analyze their data, you'd find that certain neighborhoods of Boston, nobody goes running and we know that's not true. And so, you would want to be very cautious about drawing conclusions with that absence of data.

At the same time on the research level, there may be opportunities, and this is some of the things that we want to see investigated, to be able to take advantage of the fact that the ends are so large in terms of the usage of these things. So MyFitnessPal, which is a popular food tracking App, has 65 million users. And so while there may be demographic skewing, you may want to...you may think that you've got a lot to be able to construct a reasonably representative sample within that large an "n." So, there may be opportunities there, but it's an issue now, it's an issue that should get better over time with both wider adoption and also sort of progress in methods.

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

Great. Anybody else have thoughts on that question?

Patricia Flatley Brennan, RN, PhD, FAAN – Moehlman Bascom Professor, College of Engineering – University of Wisconsin – Madison

This is Patti, I just want to add that some of the large portion of the strategy right now has focused on individual person and individual person tracking and I see some opportunities in the future for environmentally embedded sensors also being of help with this or at least sensors that are not directly attached to a person. They have issues related to identity management, certainly, but the one person, one device or one person 10 devices model is not the only one that we should be thinking about.

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

Can you provide an example of an environmentally embedded device?

Patricia Flatley Brennan, RN, PhD, FAAN – Moehlman Bascom Professor, College of Engineering – University of Wisconsin – Madison

Well, I'm actually thinking about how we've been testing temperature of people getting off airplanes right now, which is, we don't have to touch them, we hover close to them and the sensor is held by someone else.

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

Ahh, but it...

Patricia Flatley Brennan, RN, PhD, FAAN – Moehlman Bascom Professor, College of Engineering – University of Wisconsin – Madison

But there's also, I mean, you can think about, I mean the scary one is, of course, the facial recognition and the videoing of the population, which is persistent and has levels of awareness and identity management and could actually be useful for tracking behavior. In terms of internal interior environments, certainly there are many, many sensors of sensitive floors that allow you to look at footfall and pathway across the room; motion sensors and things like that. We also see a slight increase in the number of what I think of as secondarily derived sensors like alterations in temperature or noise level as an indicator of crowd gathering or of tension building.

Stephen J. Downs, SM – Chief Technology & Information Officer – Robert Wood Johnson Foundation

I could throw an example in the project I mentioned in Louisville with Propeller Health, I think in Phase 2 they're looking at adding environmental air quality sensors, sort of small sensors that can be placed around the community to be able to supplement the inhaler data with actual air quality data.

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

Wow, great, thank you. So we have some workgroup members and some staff in the queue. Linda Kloss? Don't forget to take yourself off mute.

Linda Kloss, RHIA, CAE, FAHIMA – President – Kloss Strategic Advisors, Ltd.

Yes, thank you. Excellent comments. Steve, I'd like to go back to your comment that your findings showed that there was concern for individuals on data quality, privacy, access and consent; I believe those were the four dimensions that you described. Could you say where that...is there a study that supports that? Is there more insight into details on...?

Stephen J. Downs, SM – Chief Technology & Information Officer – Robert Wood Johnson Foundation

Yes, there is. It's a study that was done by our grantee, which is a team led by Kevin Patrick and Jerry Sheehan at Calit2 at UC San Diego. The study was a combination of expert interviews and also Internet survey of researchers and of actual just users of these technologies. It is referenced in my footnote in my written remarks, which I think are part of the agenda.

Linda Kloss, RHIA, CAE, FAHIMA – President – Kloss Strategic Advisors, Ltd.

Could you just comment on whether there were any specific solutions suggested by individuals of what would satisfy them? What was the nature of their requirements or is that additional research that still needs to...?

Stephen J. Downs, SM – Chief Technology & Information Officer – Robert Wood Johnson Foundation

Well, I think solutions are to come, I think the...I mean the interesting thing we found on privacy was that when asked the question of, would you like to be able to contribute your data to research? The vast majority said yes, assuming their identity could be protected in some way. There were also nuances to that. I think there was a great quote from somebody who said, "geez, I really don't care if anybody knows how many steps I took, you know, but I kinda would be creeped out if they knew where I took them."

So, and I think that's one of the interesting aspects of these data is that they come with time and date stamps and location stamps in many cases, and there are a lot of things you can infer if you really dig into that, about an individual's behavior and what's going on in their life.

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

Great. Okay, so next in the queue is David McCallie.

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

Yes, hi; my question is similar but I'm just going to ask it a slightly different way. And it would be around what are the unintended consequences of capturing and using this data that you've thought about and if you are concerned about those unintended consequences, how you might mitigate them? So for example to lead the witness here, Steve, information about what parts of the community have health issues could lead to red lining-like behavior of folks making decisions about where to invest in that community, which would obviously, I think, be an unintended consequence of that data. So I'll just open that as a general question to all of you.

Stephen J. Downs, SM – Chief Technology & Information Officer – Robert Wood Johnson Foundation

Well certainly, that is an important one. And I think that...so the flipside of determining who is at risk for readmission and one approach to take is to really work to provide extra services to overcome the challenges that that patient might have. You know, the flipside of that is you could imagine sort of an adverse selection problem of seeking to avoid patients whose community environments are not conducive to recovery in that way. So certainly that's something you worry about.

I think in some of the other areas, things to worry about are a little bit of the, what I was hinting at in my last response, about the ability to really learn a lot by piecing together data about somebody. So you could take any of these sensors that are phone-based, a wearable that sort of know where you are at any given time, if they know where you were, you can pretty well figure out where you live, where you work, who your friends are and that sort of thing. I think there was an anecdote from the study I referenced earlier about sharing data with friends around...sharing sleep data with friends and in effect, friends becoming aware of sexual habits, as a result of that sort of thing.

So, there are a lot of unintended consequences, I think potentially around that. And I think that that's why the contract that I think people were implying that they wanted is around, use what you can for research, but I need to be personally protected as part of that transaction.

Patricia Flatley Brennan, RN, PhD, FAAN – Moehlman Bascom Professor, College of Engineering – University of Wisconsin – Madison

I want to echo something Steve said a long time ago which is, we need to also look at...this is Patti, by the way. We need to look at how we provide protection and sanctions against misuse. And they need to be sufficiently strong that the penalty for misuse would be both relevant and robust enough to cover unintended uses. I see two unintended uses in the work that we've been doing; one is inadvertent disclosure that puts an individual at a legal risk without us being able to anticipate that.

In Project Health Design, we were examining sensors in the home that with look at the amount of activity of entry and exit from the home and should there be a circumstance where Child Protective Services was involved or an individual was under a Protective Order not to enter a space and that entry could be inferred by monitoring activity, which would be done for other purposes, say for health purposes or family promotion, we could be leaving people at risk without realizing it.

The second has to do with a more general case of having people value data and inference over incite and judgment. And we tend to see this more at the interface between professionals and patients where a person's sense of not feeling well has to be complemented by a temperature of 100.2. And so, there is a, I guess it's a cultural risk of valuing precision when in fact it might be misleading.

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

Interesting.

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

Very interesting. Thank you.

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

Thanks very much. Lucia Savage?

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

Thank you, yeah, I actually have mostly a question for Professor Platt, but I would be happy to hear examples from the rest of the panel. Really interested in a little bit more specificity related to research where identifiable information about the individual is really necessary to produce the beneficial information for the public. And I know we didn't have very much time, so I really wanted to give you a chance to give me...give the listeners little bit more detailed picture of what is the beneficial output and how much identifiability is needed and a couple of examples.

Richard Platt, MD, MSc – Professor & Chair, Department of Population Medicine – Harvard Medical School; Executive Director – Harvard Pilgrim Health Care Institute

Yeah, so the basic requirement comes from situations in which data that...in which an individual's data lives in two different places needs to be put together and so you need to have an identifier to do that. And so some examples are, if you need to link electronic health record data to a state immunization registry or if you need to link maternity records to birth certificate data, it's necessary to put those kinds of information together. Do you want me to sort of go deeper into why you might want to put it together?

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

Yeah, I think for the wide variety of people we expect to be listening to this, knowing what the information is that we're trying to accomplish, obviously researchers are professional researchers, but we want it to be for the benefit of everybody, right?

Richard Platt, MD, MSc – Professor & Chair, Department of Population Medicine – Harvard Medical School; Executive Director – Harvard Pilgrim Health Care Institute

Yup, good. So here's an example from when the H1N1 pandemic influenza vaccine was put into wide use in 2009 and it was rushed into use for a much broader population than had ever been exposed to influenza vaccines. So there were sort of two new things that happened; a brand new vaccine and a much broader population who were immunized. The vaccine was administered in a whole variety of locations; in hospitals, in physician offices, in community clinics, in schools and in supermarkets.

And a substantial...and so, it was possible to identify some people who were immunized through health records and it was possible to find...to look for the potential problems with immunization in health records. But, a very large fraction of all the immunizations could only be identified by putting together these registry-based records of who was immunized with the health record so that it would be possible to track the experience of somebody who was immunized at a community immunization clinic with that person's health record that could show serious complications of having been vaccinated. Does that...

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

Yeah, so that's the key thing is that you need to know who they are to figure out who experienced a complication, upshot.

Richard Platt, MD, MSc – Professor & Chair, Department of Population Medicine – Harvard Medical School; Executive Director – Harvard Pilgrim Health Care Institute

Right. Right. Here's one that I think most people would be surprised to know but your health records say...almost never give information about whether you're still alive. So, if we're trying to assess survival from cardiac bypass surgery, we do very well at finding the cardiac bypass surgery and lots of other events, but you can't really tell the difference between the person has stopped getting medical care from the person who has died. And the best way to do that is to link to the National Death Index and to do that, you need to use full identifiers.

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

That's very helpful. I don't know if the other panelists have things they want to add, example wise?

Richard Platt, MD, MSc – Professor & Chair, Department of Population Medicine – Harvard Medical School; Executive Director – Harvard Pilgrim Health Care Institute

Well, let me just give one more example, because those are ones where the information that's transferred is the person...something happened to the person or something or something didn't. Sometimes, the second example that I just sort of showed the, you go from 1.4 million to 300 is one where you need clinical experts actually to read a section of the record, to decide...to adjudicate it.

So the example we had was a very unusual complication of immunization in infants, where a piece of the bowel telescopes into the rest of the bowel, it's called intussusception. If you just look at the coded diagnoses, you find infants who the clinicians made that diagnosis for, but since there's a lot of variation, what we needed was to have a panel of experts apply a standard set of diagnostic criteria. And in order to do that, we obtained a section of the infants' full medical record; we had individuals go through and redact identifying information and then the adjudicators got the redacted record.

So, that was an example of minimizing both the amount of data and the number of people who saw it, because some people had to actually have the fully identified data to go through it with a felt tip pen and redact all the identifying information and information that the adjudicators didn't need.

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

Thank you.

Linda Kloss, RHIA, CAE, FAHIMA – President – Kloss Strategic Advisors, Ltd.

This is Linda and I just had a follow-up example to make this point and I think the whole cancer registry function underscores the need to take the data outside of an electronic health record to do the long-term data collection, including mortality.

Richard Platt, MD, MSc – Professor & Chair, Department of Population Medicine – Harvard Medical School; Executive Director – Harvard Pilgrim Health Care Institute

Yup.

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

Yeah, I'm sure there are probably other examples of that, too. All right. So I see David, you are in the queue again; I'm going to put myself in the queue again, too. For those workgroup members who are new to the workgroup, generally we give everyone a first bite at the apple and then if there is time you can continue to put yourself in the queue so we can keep the discussion going. So we'll just continue to do that for as long as we have time. So go ahead, David.

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

Yeah, can you hear me?

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

Yup.

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

Oh good, I couldn't tell if I was on mute. This is a follow-on to the previous question to, I'll will start with Richard, Dr. Platt, and ask you, Patti made the comment that sanctions against misuse of the data is an important strategy to consider and I was contrasting that to the obviously expensive and cumbersome method of redacting all that personal information for your valuable study and wondering, do you think that if the sanctions were designed properly, that that would be sufficient enough to eliminate the need for some of the complexity and expense of the redacting process? In other words, how much of a help would sanctions be to removing the threat of misuse of identifiable data?

Richard Platt, MD, MSc – Professor & Chair, Department of Population Medicine – Harvard Medical School; Executive Director – Harvard Pilgrim Health Care Institute

I'd say there is a role for both and that the decision depends partly on how much effort it would take to do the redacting or I'll generalize it to say to minimizing the transfer of personally identifiable data. What we found is that I think many of us have been surprised about how much you can learn by...with a relatively small amount of data transfer. And so I'd say, it's worthwhile to continue investing in building better capabilities to answer important questions without having to do that kind of data transfer. And then, have the kinds of policy controls that you're talking about, that really de...sort of incentivize good behavior.

But one of my colleagues likened taking possession of these kinds of data to sort of receiving nuclear waste. Once you've got it, you're sort of stuck with it and you have to protect it forever. So, there are lots of reasons that we should make it easy, as easy as possible to answer important questions without having to do those transfers and I'd say the less you are in possession of, the better.

Patricia Flatley Brennan, RN, PhD, FAAN – Moehlman Bascom Professor, College of Engineering – University of Wisconsin – Madison

Deven, if I can speak in here.

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

Of course.

Patricia Flatley Brennan, RN, PhD, FAAN – Moehlman Bascom Professor, College of Engineering – University of Wisconsin – Madison

This is Patti. What has just been discussed refers to data that already is generated under a controlled setting, and that is the clinical care setting and so there are already some privacy preserving activities and rules that need to be followed. And there is certainly much to be discussed in that realm and I'm not minimizing the complexity of that problem.

But I also want to call your attention to the sort of Wild West of data that reveals lots about people's health and health state and health preferences and health life choices that currently lacks any formal protection, because it occurs in their everyday living, whether it's the number of times they go back to Starbucks or the amount of time I don't show up on my RunKeeper run that day because I decided not to wear it or not to get up or not to record it.

And so we really do need the privacy to turn some attention to thinking about data that is generated outside of the professional care system still poses interest, perhaps insight into an individual's health state, first of all. And secondly, the inadvertent revealing of another's health issues and health state and obviously the most common one we think about there of course is genetic information about one tells us about a whole family. But also, indoor air-quality about one patient actually discloses lots about what other people in the family are exposed to may open questions about either the need for case finding or the accountability for excess to and identifying people at risk. Thank you.

Stephen J. Downs, SM – Chief Technology & Information Officer – Robert Wood Johnson Foundation

Yeah, if I could just jump in on that, this is Steve. Patti sort of opened the door to a comment I've been wanting to make which is, if you take a social determinant's view of health and you recognize that there are so many factors, as Patti has pointed out, that influence one's health, it's hard to escape the conclusion that all data in some way is health data.

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

Umm hmm.

Stephen J. Downs, SM – Chief Technology & Information Officer – Robert Wood Johnson Foundation

You really cannot draw a line and sort of say, well no, no, no this is health and that's not health because geography is health, finance is health. Your Netflix viewing habits may speak to your mental state. There are all sorts of things that can be interpreted about health, no matter what realm of life they are in. So I think it's very hard to draw a line.

The second thing I was just going to add, sort of on the last...back to the original question which is really about the increasing ability to identify people, based on all kinds of behavioral signatures and all sorts of different data. So that's a very dynamic process, and so what seems to be reasonable redaction at one point in time, may turn out later to be easily overcome in terms of being able to identify somebody.

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

Great. Thank you all. Linda Kloss? Go ahead and take yourself off mute.

Linda Kloss, RHIA, CAE, FAHIMA – President – Kloss Strategic Advisors, Ltd.

Yes, that's right. I think that your last comments were just really in line with what I think is one of our big challenges in this whole hearing process and that is we live in a world described by HIPAA in terms of covered entities. And yet that is helping in such a narrow part of the big data world. There have been a number of discussions over the years about, is there any way to morph to kind of covered data? Can we identify what data is most...can we tie the governance to the data rather than the holder of the data? And I would be interested in your comments or thoughts on that and that would certainly apply to all three of our panelists.

Patricia Flatley Brennan, RN, PhD, FAAN – Moehlman Bascom Professor, College of Engineering – University of Wisconsin – Madison

In the absence of comments, I'll start in there for just a moment. I think the challenges really have to do with the, not only maintaining the view of the provenance of the data or letting every data element carry its access, fair use and privacy policies with it. But also in the...it's not just the metadata, but it's the data about the data, it's how often certain types of data are accessed or certain behaviors can be...knowledge about an individual can be inferred by their behavioral patterns of use.

So while I do...I think that advocating for a policy structure that has a portfolio of policies that all working towards the idea, some principles I've heard so far today, minimal access, don't hold more than you need to hold, identity only when absolutely necessary, I think will require a suite of services rather than a single privacy structure for everything. Thank you.

Linda Kloss, RHIA, CAE, FAHIMA – President – Kloss Strategic Advisors, Ltd.

Umm hmm, thank you.

Stephen J. Downs, SM – Chief Technology & Information Officer – Robert Wood Johnson Foundation

This is Steve, I think the...I think I mean it's intriguing to think about covered data rather than covered entities. I think, sort of in line with my previous comments, I think it's hard to draw the line and say what data would be covered for the reasons I mentioned, just that so many different types of data are influential around health. If I look at what the project that I mentioned in Dallas that's looking at sort of social services data and other social determinants data around assessing readmission risk, they're looking at sort of household size and housing history and employment history and social service utilization; all sorts of things that they think will affect sort of ability to kind of thrive after surgery.

I think there was a story out about a year ago; I think it was that the folks that do credit scores were going to use the same data they use to generate credit scores to generate med adherence risk scores. They felt like they didn't need additional data, you know, data that would normally be thought of as health data for that. So, I think it's very challenging to draw the line around data and call it health data.

And I think, I mean I think the other thing is it's difficult, or two other things are difficult. One is that people have very different senses, I think, of what is private to them and what they're comfortable sharing and with whom. And then the second I would add is that you may be able to...if you did draw a line around some data and say, these are the covered data, then you could probably find combinations of not covered data that could infer the covered data. So, you could get around it that way as well.

Richard Platt, MD, MSc – Professor & Chair, Department of Population Medicine – Harvard Medical School; Executive Director – Harvard Pilgrim Health Care Institute

I think...so this is Rich, I'll just say that because of that, it seems to me it's worthwhile to put the emphasis on the uses of the data and appropriate oversight mechanism. The level of oversight should be commensurate with the sort of the potential downside of the use that's made because I think it's going to be increasingly hard to categorize either the data elements or the person or the organization that holds it.

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

So what...so, I'm going to follow up on that...this is Deven. Because you just opened the door to the exact question that I wanted to ask. Harmful uses and curbing them or creating harsh penalties for people that use this data in a harmful way has come up a lot on this panel. It was also part of the White House Big Data Report. What's a harmful use? Any thoughts on how we draw those lines? Is a commercial use a harmful use, per se?

Stephen J. Downs, SM – Chief Technology & Information Officer – Robert Wood Johnson Foundation

This is Steve; you might argue that commercial use without sort of clear disclosure about the intent and about the fact that you're going to do it may well be, but I think, just sort of starting, I guess, at one point. Any sort of discrimination and denial of opportunity, you could argue. I mean, I think so often we've talked about sort of the problem with health information leading to, let's say, loss of employment or loss of insurance or something like that, so that would be a denial of opportunity. Presumably public embarrassment or embarrassment to have information that you hold very privately, to be exposed to people you don't want it to be exposed to would be another. I'd love to hear what other people think.

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

Yeah, no, me too, but can I...before we get additional thoughts on that, can I ask you to comment on the creepiness factor, too; like something that's sort of come up on...you know, in terms of in the public sensor or public discussion of sensors that are not individual but collect data across a whole stream of people, is there a creepiness issue that we should also be paying attention? And how do we define that?

Stephen J. Downs, SM – Chief Technology & Information Officer – Robert Wood Johnson Foundation

I'm not sure I have anything even quasi-expert to offer on that, other than...

Michelle De Mooy – Deputy Director, Consumer Privacy Project - Center for Democracy and Technology

Hey Deven, I can answer that. This is Michelle De Mooy from CDT.

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

No Michelle, we have to wait for your panel.

Michelle De Mooy – Deputy Director, Consumer Privacy Project – Center for Democracy and Technology

Oh, okay. Sorry.

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

So, that's okay and so it's good that we have you as a panelist because you'll get some time to either do that in your presentation or we'll be sure to come back to you with this very question.

Michelle De Mooy – Deputy Director, Consumer Privacy Project – Center for Democracy and Technology

Okay. Great.

Patricia Flatley Brennan, RN, PhD, FAAN – Moehlman Bascom Professor, College of Engineering – University of Wisconsin – Madison

This is Patti, I think there's a fairly well-known study of looking at telephone call length that was done in a small and well identified community, I believe in Connecticut; now this is going back, I think, 20 years and it began to make inferences about social behaviors, the call-to-call information of in the network versus out of the network, in the region versus out of the region. And so there was a public reporting of an overlay of behaviors about people in a particular area that was inferred by telephone records, which seems minor compared to what we can imagine now if someone's Facebook stalking of a former spouse or something like that.

There are also, in our experience again back to the Project HealthDesign, the knowledge of friend networks that is, who are your friends and are they close to you, or physically close to you, are they around you, which was one thing that was explored by one of our teams, could lead to a number of different social sanctioning and bullying and peer dismissiveness. So there's...I think there's no end to the things you could envision coming from knowing more about people than they realize that you're knowing.

But the ones that are serious, to me, are what Steve had talked about, the denial of opportunity, the denial of access that could be...could come up. And I have to say that in the last six weeks when I've spoken quite a bit about public determinants...social determinants of health in the public arena, a lot of the Twitter feed that I get, the negative Twitter feed has to do with the government knowing more about people than people want the government to know. And I think that a secondary consequence of the National Security issues, the phone monitoring and stuff, is that there is a heightened suspicion that the government is, in fact, watching your bedroom and will, in fact, make bad use of the information they have at some point in time.

And the issues seem to be less about current government choices and more about there could be some government in the future so all this will be stored and they could come back and find out that in 2014 I overslept 10 days, because you could tell from my Fitbit that I wasn't at the gym. Thank you.

Richard Platt, MD, MSc – Professor & Chair, Department of Population Medicine – Harvard Medical School; Executive Director – Harvard Pilgrim Health Care Institute

It seems to me...this is Rich. It seems to me there is unlikely to be a closed form answer to this but there would be a fair amount of protection or comfort to be gained...that's the wrong term. There should be a fair amount of confidence to be gotten by ensuring that the uses are disclosed publicly and that the oversight mechanism includes a fairly broad representation of the community that's likely to be...whose data is likely to be involved.

Stephen J. Downs, SM – Chief Technology & Information Officer – Robert Wood Johnson Foundation

This is Steve; let me just throw one thing back to Deven, your question about creepiness which is that, I would argue there is a very fine line between a beautifully personalized tailored service and creepy. So many of the things that we've come to appreciate in this sort of data enriched world are the result of companies being exquisitely designing service to take advantage of the knowledge that they have about you at the time. So knowing where you are to inform your query...the answer to your query better or knowing your habits to know what you're more interest in or less interested in. These are things that people value very much. And I think, obviously you get a little to the wrong side of that and it doesn't feel good at all.

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

Terrific answers. I appreciate it. All right, Lucia, you're next.

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

Yeah, I want to go back to the so-called mosaic effect, so that's when you have two data sets and you combine them and it starts filling in more information than each data set on its own would be indicative of and it's through that mosaic effect that you do this exquisite tailoring or this harmful discrimination. And so my question for Patti and Rich is, based on what you know and your experience, particularly in the academic realm, are there policies or steps or processes we can leverage and take out of academia and bring into these other realms that help us confine mosaic effect type activity to things that there is a public consensus about it being beneficial? Or prevent it from being used in harmful ways? Like what are processes that might...oversight mechanisms, whatever, that we could migrate from academia to these other settings where people are doing data analysis? If any?

Patricia Flatley Brennan, RN, PhD, FAAN – Moehlman Bascom Professor, College of Engineering – University of Wisconsin – Madison

One process I don't want you to migrate is the confusion of IRB and HIPAA accountabilities, because that has really, really been a very bad thing and has had some very bad outcomes. On the other hand, I believe that the idea of discourse about the anticipated and unanticipated impact of data use is something that can be extremely helpful and just as we've seen the rise of data safety monitoring plans in research proposals now; it's unusual to have a big proposal that doesn't have a clear data safety monitoring plan. I see the expansion of that concept of data safety monitoring to include a real challenge to the proposers that they anticipate and bring forward and speculate intentional and unintentional uses of their data. So I guess I see two things that would be important, one is to start to empanel people as well educated about potential discovery and disclosure that can happen through data mashing in a way that they serve as a good public review board of it.

And secondly, to look at the process of grant funding, which is where a lot of academic research continues to be generated from and call for an expansion of the data safety monitoring plan to also request the data anticipated uses plan. As we see the growth in journals that are now asking individuals, asking office to deposit the data that led to the conclusions of the paper, we have a real responsibility to expand the idea of data safety monitoring to data use anticipated use effects. Thank you.

Richard Platt, MD, MSc – Professor & Chair, Department of Population Medicine – Harvard Medical School; Executive Director – Harvard Pilgrim Health Care Institute

Right, so I'll add that it's possible to put quite sophisticated controls on the uses of the data and the users of the data so that to the extent that we could agree on what an appropriate use is, even if it's on a case-by-case basis, say a question can be asked of certain data only with agreement of an appropriate oversight mechanism. It's pretty straightforward to build in controls that would require that kind of approval before the data could actually be used.

Deven McGraw, JD, MPH, LL.M. – Partner – Manatt, Phelps & Phillips, LLP

Okay. Terrific, thank you. We have a little bit of time left. Lucia, do you...you said you have another question, do you want to go ahead?

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

Yeah, it's not a follow-up question, which is why I don't want to take away from somebody else who's already in queue, but if there's nobody in queue, I will definitely ask my question.

Deven McGraw, JD, MPH, LL.M. – Partner – Manatt, Phelps & Phillips, LLP

Yeah, I don't see anyone. Oh, hold on.

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

Go ahead, I'm sorry, I was raising and lowering, this is Stan Crosley. I was going to have one quick follow up question.

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

Let Stan go first Deven, I'm going to go back on mute until you call me.

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

I'm sorry to interrupt, but so the last comment on, and we could potentially control appropriate use on a...it could be almost ad hoc or anecdotal as they arise and we could control questions asked of certain data. I think that works, and I'm not sure if that was Rich or Steve, it sounded maybe like Rich.

Richard Platt, MD, MSc – Professor & Chair, Department of Population Medicine – Harvard Medical School; Executive Director – Harvard Pilgrim Health Care Institute

Yeah, it was Rich.

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

I think that works really well on a controlled data set. I think back to Patti's perception of the data that's getting generated from all different places, and Steven's comment as well on the social determinants; I think that's going to be an extremely difficult thing. Now, I like the idea of trying to set that framework but beyond the kind of the controlled data sets, is there a framework you could...the three panelists could think of that could start to generate, you know, we have harmful use or is there an appropriate use frame that you could start to think about? It's an easy question.

Patricia Flatley Brennan, RN, PhD, FAAN – Moehlman Bascom Professor, College of Engineering – University of Wisconsin – Madison

I haven't heard this come up in the discussion, yet but one of the factors that I think has to be considered carefully is whether or not an entity can make financial...can gain financial value out of the use of the data...of data from an individual without their knowledge. Now, I understand this certainly is happening now, anyway, but as we move into this era, it might be a time for us to be able to say that...to put forward, or at least posit a policy that requires any financial gain to be shared with the data contributor or something like that. And I realize it's unusually complicated to figure out how to do it, but increasing...

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

I'm sorry, when you say share, you mean disclosed or literally shared?

Patricia Flatley Brennan, RN, PhD, FAAN – Moehlman Bascom Professor, College of Engineering – University of Wisconsin – Madison

I actually would like to go to literally shared, but I think that, returning the \$1.25 from my RunKeeper every month is probably not going to be financially viable. But I certainly think at a very minimum, publicly disclosed and, I mean, I could really see, and we saw this fear being raised originally with genetic data and were reassured it wasn't going to happen and the Henrietta Lacks book came out, so there's...to trust the marketplace to treat personal contribution, thinking as a public good into a private leveraging seems to me to be something we can no longer consider.

And there may be models that come from other areas, I'm thinking of a donation, where there's an active...an act on the part of the individual that gives over a substance that is known to have other uses, some of which may be commercialization. So I just want to put it as a placeholder that it would seem to me excessive financial gain and perhaps potentially restricting access to my data is something that I would find it a serious violation.

Stephen J. Downs, SM – Chief Technology & Information Officer – Robert Wood Johnson Foundation

This is Steve, just a couple of thoughts and you're right, it's a very, very hard question. Part of what I'm thinking about and I know you've got John Wilbanks on the committee there, is a little bit sort of thinking about how creative commons went, sort of took the very binary active copyright and added nuance into it, but not so much nuance that it was unworkable or confusing. And so it might make sense to think about a framework that allows those people who generate data about themselves to be able to sort of select and dial up, dial down sort of different uses. And also just recognize that there are probably, or I would say undoubtedly, some uses that no one should be able to consent to because they're just flat-out wrong, you know, and active discrimination that we talked about earlier may be falling in that category.

But I like the idea of a framework that gives people control. I think too often we take positions of sort of outright protection without the ability for people to make trade-off decisions and sort of trade-off benefit for risk. So I think if you center something around individual control and then a reasonable number of things that they could agree to, based on fair disclosure about what they really are.

Richard Platt, MD, MSc – Professor & Chair, Department of Population Medicine – Harvard Medical School; Executive Director – Harvard Pilgrim Health Care Institute

So this is Rich. I find the individual control piece is...it has lots of advantages and some potentially great disadvantages, at least in the realm of the kind of work that we do, for instance for FDA. It's really essential to have confidence that we're evaluating sort of representative groups of people. And if there's sort of individual opt-out, we can easily sort of lose that ability because the people who are left may be systematically different and so we'd come to a very wrong conclusion.

Stephen J. Downs, SM – Chief Technology & Information Officer – Robert Wood Johnson Foundation

Rich, this is Steve, that's a great point and I wonder if sort of on the one end of the spectrum were the things that should not be ever done, maybe there's also a range of information that should not be opted out of as well.

Patricia Flatley Brennan, RN, PhD, FAAN – Moehlman Bascom Professor, College of Engineering – University of Wisconsin – Madison

Oh, interesting.

Claudia Williams, MS – Senior Health & Health IT Advisor - Office of Science and Technology Policy – White House

This is Claudia, I'm from OSTP. Sorry, we can't raise hands because we are blocked from the website. But I've heard patient groups talk about the concept of a social compact versus permissioning and consent being the only...where I say these are the ways in which I want you to derive benefit for me and others like me using my data. And I'm just wondering how that fits into this conversation and whether you could see that...I like where things are going in terms of like things you never do and thinking about individual control. But I'm just wondering about this concept of kind of the give and take and what I want in return, whether that's financial or that you'll publish the results openly or whatever that might be.

Richard Platt, MD, MSc – Professor & Chair, Department of Population Medicine – Harvard Medical School; Executive Director – Harvard Pilgrim Health Care Institute

Yeah, that makes a lot of sense to me to say, first of all, we'll always...it will always be clear what use is being made of data and there is an opportunity both before and after to assess the appropriateness. If it's before, you could say, this is or is not appropriate and after the fact you can say, we've learned something important about whether or not to use these kinds of data this way. And I think that that process should include healthy representation of the people whose data are being used. But that's different from each person has individual control over whether the data are used or not.

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

Yup. Thank you all very much. So, Lucia, I don't know if that was where your question was. We are a little bit over time, but if it's a quick one, I think we'll squeeze it in.

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

I'm going to save it for another panel, I've got it planned out already, and so, it's okay.

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

All right, well terrific.

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

And I need a break, just like everyone else, so...so much great stuff to absorb.

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

Yes, oh great. No, this was terrific from all of you. We have another panel coming up. We...on the agenda it starts at 2:30, but we...2:30 Eastern, we ate a little bit into our break, so, I'm going to see if we can start at 2:35 Eastern, does that make sense, Stan?

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

Yup, that's fine.

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

Okay, we'll eat a little bit into the next panel, because we do have...well, at any rate we'll do our best to make it up on the back end. So, everyone be back by 2:35, Stan will start us up with the next panel promptly. Thank you.

Okay, it's Deven; I see 2:35 on my line.

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

You're so prompt all the time. I do, as well. So we can...or make sure our panelists are back for the next panel, is going to be on Health Big Data Concerns and we have Michelle De Mooy, Mark Savage and Anna McCollister-Slipp. And hopefully they're all three on.

Michelle De Mooy – Deputy Director, Consumer Privacy Project – Center for Democracy and Technology

Yup, I'm here.

Mark Savage, JD – Director of Health IT Policy & Programs – National Partnership for Women & Families

This is Mark and I'm on.

Anna McCollister-Slipp – Co-Founder – Galileo Analytics

This is Anna; I'm here.

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

Okay, great. Well let's go ahead and get started. Our first speaker is going to be Michelle De Mooy and Michelle is the Director of Consumer Privacy Projects for the Center for Democracy and Technology. Michelle, please go ahead.

Michelle De Mooy – Deputy Director, Consumer Privacy Project – Center for Democracy and Technology

Thank you. Actually Deputy Director, I should correct that. Thank you so much for the opportunity to testify today. I'm just going to jump right in. The healthcare industry, like a lot of other sectors, has been facing a lot of exciting opportunities as a result of big data. Healthcare providers, insurers, pharmaceutical companies and many others are applying advanced analytics to large and disparate data sets to gain valuable insight on treatment, safety, public health and efficiency, overall. The increased uses, as other panelists have mentioned of mobile Apps and wearable devices have also given rise to new healthcare applications.

As people are increasingly sharing intimate details on their health and wellness, individuals are leaving a huge digital health footprint in many places, including some that they may not expect such as online searches. A person's health footprint now include these searches, social media posts, inputs to mobile devices and clinical information such as downloads from implantable devices. Much of the privacy and security challenges, or many of the privacy and security challenges facing traditional healthcare providers in the big data era also apply to App developers and wearable device manufacturers. Notice and consent, for example, is a difficult problem. Security is a critical issue for developers and device manufacturers, just as it is for clinical providers.

But there are major differences and probably the largest is the incentive structure for actually implementing user privacy and security. HIPAA, while not perfect, does not apply to most App developers or device manufacturers and so this sector lacks this regulatory framework that applies to clinical providers. And without clear ground rules and accountability for appropriately and effectively protecting user health data, these entities tend to become less transparent about their data practices and also about crucial mechanism such as algorithms, crucial decision-making mechanisms.

We believe the Fair Information Practice Principles offer some guidance here. I know that there's some debate about whether they work still in this era, but we think the flexibility and rigor of them provide an organizing framework that offers important parts of this puzzle, such as data governance, innovation, efficiency and knowledge production while also protecting patient privacy. We believe that the best approach for data in the traditional healthcare system is to start with the FIPS based rules under HIPAA and the Common Rule and interpret them for big data uses. This effort could further benefit by laying a groundwork for a consistent sets of principles covering both this traditional healthcare sector and emerging consumer applications, which is where we are focused right now.

Just briefly, security...data breaches, of course, remain the most pressing security issue in big data healthcare. The steady increase in attacks from outside and inside organizations continues daily as is the number and sensitivity of the record accessed or stolen. And of course the ACA has increased enrollments for health insurance and has attracted more hackers and it's leading us down a road with more...larger and more invasive healthcare breaches.

So, one of the concerns that we've identified is that patient records are often stored in data centers with varying levels of security. Even with HIPAA certification, these centers usually are often struggling under the weight of the storage and processing of this voluminous data that are coming in from multiple different sources. The variety of the data formats and sources makes it almost impossible for them to apply traditional security standards.

De-identification is a useful tool but it can't be presumed to eliminate all risk of re-identification of a patient. Therefore it's important to require assurances from recipients of de-identified data that the data will not be re-identified, as discussed previously, and to provide penalties for re-identification.

Other core security activities or core measures we think include creating a common parlance or common representation through data varieties. One example would be in the body Sensor network data. Real-time risk analysis and threat modeling is another critical way for entities using health big data to get ahead of breaches.

Privacy has been discussed quite a lot so far, so I'll just boil my comments down to this. Big data is dumb. The volume of health data contained in electronic systems is vast, but the large majority of it is all over the place, fragmented and hard to see. It is spread out among providers, researchers, insurance, state and Federal governments, all with separate rules, laws, ethics and motivations. The need for interoperability between systems and policies is as much a privacy issue as it is a technology issue. With so much data floating in and around clouds, all over the place, purposeful or inadvertent privacy violations are almost inevitable and it's very costly for individuals and businesses.

Dumb data insights the creepiness that Deven mentioned because it confuses correlation with causation often and defies consumer's expectations. Algorithmic transparency is crucial, we think. Many companies have entered the health data space and they consider their models proprietary and refuse to reveal them, which leaves a gaping hole where our understanding of these decision-making mechanisms should be.

And in conclusion, building and maintaining public trust in a broader, robust health big data ecosystem is going to require development and implementation of comprehensive adaptable privacy and security policy and technology frameworks. We think those frameworks should apply to health data regardless of the type of entity that's collecting it, be it a hospital or a commercial health App and yet still be flexible enough to respond to the particular risk to privacy posed by different health data sharing models.

We think it should include mechanisms to hold entities collecting and analyzing health data accountable for complying with rules and best practices. We think it should provide incentives for the adoption of privacy enhancing technical architectures or models for collecting and sharing data. And we think it should be based on thoughtful application of the Fair Information Practice Principles. And that's all I'm going to say for now because so much of what I had planned to say was sort of already discussed.

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

Stan, I think you are on mute?

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

Yeah, but I was brilliant while I was on mute. I was just saying thank you, Michelle and you will have plenty of opportunity to explore that in the question-and-answer session, so thanks again. Move to our next panelist is Mark Savage, and Mark is the Director of Health Information Technology Policy and Programs for the National Partnership for Women and Families. Mark, welcome.

Mark Savage, JD – Director of Health IT Policy & Programs – National Partnership for Women & Families

Thanks very much and I did have a short slide deck for use with this.

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

Great.

Mark Savage, JD – Director of Health IT Policy & Programs – National Partnership for Women & Families

And if you can move to slide number three, please. So I thought it might be useful to share two communitywide conversations that I've observed on health big data concerns and solutions. Hopefully, this will also give you a wider frame of input, not just mine.

The first one was a recent conference on big data and civil rights. It was hosted by Data and Society Research Institute Leadership Conference on Civil and Human Rights and New America's Open Technology Institute. It covered a broad range of topics; health was one distinct one, but it also covered education, criminal justice, employment, finance and housing. So, the big data issue is a broad one in the civil rights community. And it brought together a broad mix of leaders across the nation to discuss the issues.

There were two distinct issues that were sort of at the forefront of the entire day. The first was privacy and the threat that greater surveillance poses for low income communities and communities of color. And that was...surveillance was both seen in the collection of big data, but also in the analysis of big data. And the second large issue, and this is in the health context as well, was health disparities and the promise of big data to assist population health leaders in identifying, analyzing and addressing health disparities. You can go to the next slide, please.

In this conversation and I'm just focusing on health big data, there were some broad themes that emerged among all these discussions. First, the same piece of data can be used to reduce health disparities and empower people or conversely, to violate privacy and cause harm depending on who holds the data and what the person does with it. This was a theme throughout the day and there were some...I have given some examples here. Greater demographic granularity can be used to help address health disparities or it can be used to increase the risk of profiling. Information about whether one has had a vaccination could be used for a public education campaign or it could be used for targeting increases in insurance premiums. So you have this same data being used for different purposes, depending upon who holds it and what they might be doing with it.

Also, there was a lot of discussion about what is health data, what are the sources? And one of the themes that emerged is that all data can be health data or, data from which inferences about health are drawn or correlations with health are made. And lastly, a theme was to focus on uses and harms rather than cost and benefits. The conclusion was that talking about cost and benefits implies trade-offs and didn't want to necessarily be put there in saying that if the benefit was greater than the cost then it was okay. So people thought we really should be focusing on harms and uses and to do so, also allowed us to seek redress through civil rights laws. So this was the first sort of communitywide conversation to share with you for your thinking. If you can go to the next slide, please.

The second conversation was a conversation back in 2010, when I was in California and we convened some of the leading health privacy and community organizations in California, and even in the nation. You see some of their logos up there. We took a full day to discuss these very issues in the broader context of health and health information exchange. I have to say, it was a very rich conversation, a transformative conversation, even.

And there was one particularly memorable moment where a privacy advocate was talking about the importance about individuals being able to withhold their information, health information, and to consent or not consent. And when another person around the table heard that, a person who is a leader of the health organization in a community of color, the person looked astonished and said, but if you do that, then the community doesn't have information that it needs in order to identify and address health disparities. So this was not sort of an adversarial conversation and I'm not mentioning this for that purpose, just to lift up the range of perspectives around the table on a very important question. If you go to the next slide, please.

Here's what the group came up with, not only in the course of that day, but in the course of sort of six months afterwards of looking at principles for health information exchange. And I've just summarized them here; I provided the original document as a background for the workgroup to look at it, at its leisure. But comprehensively the group identified that there should be benefits for personal health. There should be benefits for population health, for the community, for research, and this is often where the big data question is raised. It should be the case that all patients and consumers are benefiting fully and equally.

The fourth principle was what we often nicknamed universal design, that we should design the technology and services to meet the range of needs without barriers for some. Fifth, and equally important part, but a part was ensuring privacy and security of health information and there was...you'll find in your background attachment that there was also extensive reference to the Fair Information Practice Principles, as well and the recognition that there are many tools for protecting health...for protecting privacy and security, not just consent.

And six, and I'll sort of stop here, was the principle of preventing misuse of patients data. And what I lift up there was we had a discussion about the affirmative uses of health information exchange and gathering health information. But, we also recognize it's important to add some prohibitions, the things that you cannot do and that both sets of lists, together, may help us carry the effort further. So with that, I'll close with my opening remarks.

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

Appreciate that very much. Okay. And now, our final panelist is Anna is McCollister-Slipp, Co-Founder of Galileo Analytics. Anna?

Anna McCollister-Slipp – Co-Founder – Galileo Analytics

Hi there, thank you so much. It's truly an honor to be included in this panel and in this workshop, or in this workgroup hearing. I have some slides, could you go to the first one? So I wanted to start with a little bit of context as to why I'm here. Four, almost five years ago, I took my BA in journalism and my background in public affairs and cofounded a company that does visual data analytics of big health data. How does something like that happen, I mean apart from being a nerd and having a little bit of chutzpa, I was incredibly frustrated as somebody who lived with Type 1 diabetes for at that point, I don't know, a couple of decades, who had very difficult to control diabetes, had all of the complications that come with diabetes such as eye disease, nerve disease, kidney disease and I found myself in several occasions as a true outlier.

But an outlier and individual who was...for whom...I had a difficulty accessing certain types of drugs or getting drugs paid for, based on the results of randomized controlled trials that had inclusion and exclusion criteria that screened out people like me. So I was excited, excited enough to cofound a company that does visual data analytics, at the prospect of all of the data sources coming online from electronic health records and claims data to patient-generated health data such as that that I generate through my diabetes devices.

And thought that finally, we would have the infrastructure and capability necessary to be able to do real-world examination of health data and to come up with meaningful ways of understanding smaller and smaller, more refined cohorts of individuals, and that we would be able to develop policies, whether it's approval, whether we come up with better outcomes for drug approvals or whether we come up with better ways of understanding the benefits of certain drugs or treatments for smaller patient cohorts. I thought big data was a very exciting as an opportunity for all of us, as individuals, as a society and as a healthcare system.

If you could go to the next slide, this is a slide I present quite a bit when I talk about some of the dysfunction, the data dysfunction that I live with in my own care with Type 1 diabetes. This kind of represents my ongoing day-to-day, week-to-week, month-by-month regimen with Type 1 diabetes and the complications. If you can see, in the lifestyle area I've got stress management, nutrition management, sleep, strength training, cardio, I take walks, I use fitness trackers, etcetera. So that's one thing, that's stuff, what everybody has to do.

If you look at the yellow bubbles, that represents the physician appointments I had. In 2013 I saw 13 different physicians for total of 63 different doctor's appointments. I have medication; I take 15 different medications per day. For lab values, there are like 132 different lab values I have done every three months so that I can access my drugs. I follow 15 or so pretty closely because it tells me important things about the status of my health and my complications from diabetes. And I use a multitude of devices, some prescription, some not.

All of this generates data in one form or another, much of it could be incredibly helpful for me personally, if I could combine the data in a meaningful way and to a single data string that represents...would enable me to just look at patterns between...patterns in my own experience that would be visible if the data streams were in one spot.

But, I can't do that. There are all sorts of roadblocks that keep me from doing it and much of the frustration that I have is that I see this and I see this as an opportunity for me to have better care for myself, but I also see this as an opportunity that if we could get this kind of data and access it and aggregate it, that we'd be able to have a far, far better understanding of what really is relevant and matters to individuals such as me, who have very complex disease. We'd be able to do far more...we would be able to develop far better outcome measures than something like hemoglobin A1c, which is a pretty anemic outcomes measure for those of us with complex Type 1.

So, this is where I am, I think this is where many patients are at the moment. We've got this data, it could be incredibly valuable, we're kind of drowning in it, but none of it's particularly useful. And one of the big reasons that I am constantly told when I speak in places about this and when I talk to device manufacturers or hospitals or labs, lab company representatives, one of the biggest burdens is privacy, or at least the perceptions of privacy and security. And I'm a little suspect that some of those claims are actually valid, but the laws...our understanding of HIPAA is so complex and in many respects opaque, even for somebody who is as nerdy as I am, that it's very difficult to refute many of these claims.

So for me, and I don't mean to belittle concerns about privacy, because it can get a little creepy at times, but for me, I see privacy as a true barrier and security is a true barrier; not that they're not important, they certainly are. But our overemphasis on it has kept us from being able to reap many, many benefits from the data sources that we're all generating. So, if you could go to the next slide.

I would say we have a very urgent need for data liquidity, both for clinical use, for individual use, but also so that we can access and create the learning health system that we ultimately need. Next slide.

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

And Anna, we're going to have to have you wrap up pretty quick.

Anna McCollister-Slipp – Co-Founder – Galileo Analytics

I'm going to be very fast.

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

Okay.

Anna McCollister-Slipp – Co-Founder – Galileo Analytics

Essentially, those who need access to data can't get it, whether it's me, my physicians, caregivers, entrepreneurs who want to develop innovative applications to it, but ultimately, researchers who want to do the kind of research that I think we all need. And even regulators who are looking for safety signals or things we should all be concerned about. Next slide.

Ultimately, what I've discovered is that the people who have access to the data won't share it, whether it's hospitals and health systems or HIEs, the data aggregators or brokers, Pharma companies, insurance companies; all of these companies have access to large stores of data but they keep it siloed and separate from and they charge large amounts of money for access to that data.

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

Just a concluding statement from you then maybe, then we can come back on some questions and answers, Anna.

Anna McCollister-Slipp – Co-Founder – Galileo Analytics

Yup, if you go to the last slide, it's right there. So, there are a lot of reasons that are given for why there is a lack of data liquidity but ultimately, I would say, that it's a lack of a sense of urgency, it's a failure to understand that if you have data, that it's a social asset and that you have a degree of social responsibility to give back to the community by making the data available to researchers and to patient groups. And ultimately I think it's a failure to respect patient's needs, the intelligence or the sacrifice that every individual makes when they go through the process that ultimately creates each of those individual data points.

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

Thank you, that was tremendous. And thank you, each of our panelists, that was a great opening to this session and I've got a number of questions, but I see some of our workgroup members and I want to make sure to go there, first and we'll cover the bases, any questions I have. So I'm going to open with David McCallie, I see you in the queue.

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

Yes, thanks. My question is rather narrow and maybe it's something that should be followed up in some other setting, but I'll just give Michelle a chance to say a few more words about her comment on the need for algorithmic transparency. And I'm just curious as to what kinds of algorithms and what kind of transparency were you thinking of?

Michelle De Mooy – Deputy Director, Consumer Privacy Project – Center for Democracy and Technology

Sure, yeah. So, the best example I can think of is probably Google, right, and I feel bad because they get picked on a lot. But Google has a search algorithm, so it's assuming people don't know what this is because this is sort of the geeky thing that I do, it's a mathematical equation. And that equation evolves over time and it's sort of a learning system similar to what we'll discuss later.

And what these algorithms do is they take information and they contextualize it and they spit information back. So in other words, when you put a search into Google for a health diagnosis, it will spit back the information that it thinks you're looking for. And so what's happened over time is algorithms have become extremely sophisticated and nuanced to the point where they are sort of replacing, shall we say, human decision-making processes. So there's not a human behind those search results, there's an algorithm and that's the case for a lot of different types of applications and services.

And so what we've been looking at is how different types of decisions are made by these algorithms and how the algorithms themselves are designed. So, a couple of interesting thoughts on this have been, do the people designing the algorithms affect the decisions that they make? So, if you have somebody from a community of color who is designing an algorithm, a decision-making algorithm, does that impact the decision-making process? Or, does being a male or a white male impact the decision-making process?

But, the issue, and one of the biggest problems in this space, is that many, many companies consider these to be proprietary. In fact, Google is quite open about many things, but will not share this; it's sort of their secret sauce, I think, in their minds. And so, understandably, they feel a proprietary interest in them. But without that information, it's very difficult as a privacy advocate or anybody, to be able to look at what the inputs and outputs are that are making decisions about you. In other words, if someone has decided that you look like, based on a facial recognition print and marrying that with public data with your ZIP Code and perhaps a search looking for a health diagnosis, that you should be prescribed this type of drug. Or, that you are this kind of person that should be sent advertisements about this type of product.

In other words, let's say you're an African-American male who lives in a poor neighborhood, you walk into a CVS, your face is biometrically canvassed and printed and may be not identified, but an algorithm will take all of those together and perhaps say, there is a high percentage indication that this person might have one of these types of illnesses and therefore should be prescribed this type of medication, or offered a coupon for it.

Anna McCollister-Slipp – Co-Founder – Galileo Analytics

This is Anna and I, as a consumer, I would say that's ab...I couldn't agree more wholeheartedly. I mean, it's absolutely critical, not only should the data be available so that people could do counter-analyses and be able to divine their own cohorts, but we should know exactly who is using it and for what. And there needs to be a lot of transparency and disclosure, not just about algorithms but about what informs the algorithms, how that cohorts are defined and how individuals are separated. If that's opaque, if we can't access the data and if that process is opaque, then nobody will ever trust the system; you would have no reason to.

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

Great.

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

Well, we could have a big discussion on that subject, but I'll defer to other questions from the members.

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

Yes. Let's go to Linda, she has a question. Linda Kloss?

Linda Kloss, RHIA, CAE, FAHIMA – President – Kloss Strategic Advisors, Ltd.

Thank you and thank you to our panelists. My question is I think directed at Anna, but certainly others' perspectives would be really helpful. We talk about privacy as a barrier that's used as an excuse for not merging data or making data available. To what extent is it your impression that part of this issue is still the lack of understanding about our privacy framework and the rules misinterpretations, using it as an excuse or a barrier? To what extent do you perceive that we really understand how to live within the current privacy framework?

Michelle De Mooy – Deputy Director, Consumer Privacy Project – Center for Democracy and Technology

I think I'll take a stab at that, so sorry, just really briefly. I think something that industry forgets a lot when they're arguing that privacy is bad for business is that in fact the Internet is a privacy innovation, right? There was a point in time where people who are my age might remember when people were afraid to use it at all to do any kind of transactions. The privacy innovations moved it forward. And that's the case with health data. It would make big data smarter, more targeted, it actually would, of course, embolden the public to trust more big data systems and attached to the public understanding is the transparency but also the communication, just in general, about what is happening to data. I think one of the hardest things for people to correlate is, I'm putting my data into this machine and the fact that it could come back in some way to profile them in a negative way is really difficult for people to conceptualize or understand, it's a really complicated process. So part of it is the transparency but also the communication about what privacy means and how it actually helps you manage information. And just the fact that people think that for example HIPAA really covers all medical data and have really no idea or understanding that it doesn't in a lot of circumstances.

This is also true, these people are also people who are making Apps and so there's a lot of outreach that also needs to go along with that back at the industry to help kind of younger startups and people who are getting into the health big data space understand what ethical and responsible data use looks like.

Anna McCollister-Slipp – Co-Founder – Galileo Analytics

And this is Anna. I mean, my experience is truly anecdotal but I do a lot of speaking about related subjects and I feel, I mean, I don't understand what HIPAA is; I think I have a pretty good understanding compared to other people but it's really difficult when you're talking to a device manufacturer about why they won't open up their API or you're talking to the CIO of, I go to a big research, academic research center in Washington and talking to the CIO about the fact that I still can't get the patient portal to work. I mean, I start citing a variety of things, including privacy and security. I mean, who am I to push back, I'm not a HIPAA attorney or a privacy attorney and I just feel like the overemphasis on that is a significant issue, sometimes becomes an excuse for a lack of progress.

Linda Kloss, RHIA, CAE, FAHIMA – President – Kloss Strategic Advisors, Ltd.

Thank you.

Mark Savage, JD – Director of Health IT Policy & Programs – National Partnership for Women & Families

This is Mark; can I throw in one additional thought...

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

Absolutely.

Mark Savage, JD – Director of Health IT Policy & Programs – National Partnership for Women & Families

...which is, in the conversations that we had back in 2010, a theme emerged which was that this is not really an inherent tension between privacy and use of data that consumers actually want both; they want their privacy and security protected and they want their information exchanged and used properly for health purposes. And the thought was, we have the tools for doing both, and that was part of the underlying idea behind the principles as they articulated them back then. And I think it's helpful to try to say, how can we accomplish all of the proper goals that we're trying to accomplish and not say it's a choice between one or the other?

Anna McCollister-Slipp – Co-Founder – Galileo Analytics

I would agree with that, I'm not trying to say that privacy isn't important, I'm just saying that there are other things that are important as well and that we can't let coming up with a system of perfect privacy be the enemy of making progress. And as somebody who has been advocating about this issue for the past five years, trying to get better access and be...to my own personal data, let alone being able to access aggregated data sets. It seems to me that it's become more of a barrier than it actually warrants.

Michelle De Mooy – Deputy Director, Consumer Privacy Project – Center for Democracy and Technology

I think one thing I would add to that is just that in a government context, I think there's a lot of confusion. There are a lot of different rules and regulations that go around. What the federal government can do, what state governments do and then of course, what local and municipal governments do, even leave comes to something that you would think would be more clear cut, like public health. So I think that's a clear space where perhaps the messages of privacy being a barrier are hitting too close to home and where some state health centers aren't releasing data when they could be, they just need to understand a responsible roadmap, a way to do that.

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

I suspect that Deven has a question that's running along this theme as well. Deven?

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

Yeah, it is, although you started to circle around answering it. I think I want to get to a combination of what I think really each of you has raised, which is this issue of undoubtedly we need a trusted way to accomplish the data sharing that is necessary to enable individuals to take care of themselves, to have their own data, analyze it, contribute it to research and how to be used by researchers, you know, the sort of data for the good that I think we could at least clearly define some categories are, while still having privacy protections.

And I just want to push on this a little bit and I'm wondering whether what you may be...I don't want to put words in your mouth, I guess I want you to react to the following thought which is, because you want both, privacy and security as well as data flow, if you can't have the absolutes of either because that's where you start to have the trade-offs and we might actually have the, whether due to perception about what the law says or what the law actually says, have the scale tilted more to one than the other.

Is there an argument that the data...that privacy protections that create obstacles to the good kinds of data flows that we're trying to encourage, that that's not what we should be focusing on and in fact, that's over privacy at the expense of the kind of, you know, possibly to the detriment of being able to yield opportunities from it, you know. So consent, for example, just to put it on the table, is one of those issues that if you require it to be obtained before you can make a good use of data, that that might be an obstacle.

Another example might be, if you have a difficulty when a patient asks for information being absolutely certain that the person on the other end of the telephone who's asking you for the data or who pings you by email is the person who they say they are and you make somebody jump through a gazillion hoops in order to say who are because we don't have a national identity system. So apologies if this feels a little all over the place, but is there a litmus test for some of these protections where even if they were well thought at the time, they're creating obstacles, that that's sort of an argument for removal or modification?

Anna McCollister-Slipp – Co-Founder – Galileo Analytics

That's the sense that I have...this is Anna, that's the sense that I have. I mean, and again I'm not trying to represent myself as a privacy expert, I know other patient advocates have focused more on this issue but I can say that I, as somebody who has had a vitreous hemorrhage because of the complications of my disease, or I've got ongoing complications that I have to manage, being able to access all of my data in one, coherent data stream in one place, could have very specific beneficial results for me today, tomorrow, next week that could keep me from having a very difficult, potentially blinding, adverse event or complication. And I don't have a lot of patience for the fact that five years after I started my company because this was a great opportunity in terms of like potential for what we can learn from big data, I don't have a lot of patience for the fact that I can't even get my own data, let alone...from my hospital physician portal or my own devices in one place. And it drives me crazy that the reason that's given is privacy.

I mean, I don't pretend to be representative, I'm obviously talking about this stuff and just displayed my entire medical regimen in public through this forum, but at the same time, I don't think I'm all that different from other people and if you look at some surveys of both physicians and consumers around this issue, the majority of physicians and consumers actually are less concerned about privacy than we're led to believe.

Michelle De Mooy – Deputy Director, Consumer Privacy Project – Center for Democracy and Technology

Yeah, actually I would pick a bone with that just a little bit that there's a survey that Pew did and they always do pretty interesting stuff, and one of the things that caught my eye was that the second kind of data that people are most concerned about was health. And now on the same token, you hear a lot of surveys where really want to contribute their health to research etcetera. So I think, Deven, I think that's...it's the question that HIPAA was trying to answer and ended up being sort of almost like a use case specific sort of law. And I think in a way that is the troubling part, that's the difficulty. I know that a lot of threat models have been developed that can be useful.

And again, I don't know how sort of burdensome that would be, but there is potential there for individual and community threat models and risk models where companies can take a look at the flows from start to finish and assess where the risks would come in for violations of privacy or security and try to build in preemptively to try to stop that.

Mark Savage, JD – Director of Health IT Policy & Programs – National Partnership for Women & Families

So, this is Mark; I would say I think the existing privacy laws that we have, as I've looked at them, have provided a pretty good framework for things, speaking broadly the focus on exchange for treatment, payment and operations, the use of limited and de-identified data sets for larger aggregate purposes. I think what we haven't done as well is in the, and turning to the principles, is prohibiting the misuses of data. So it's been mentioned before, there really should be a prohibition against re-identifying data. It won't prevent that as it's not a physical barrier to doing it, but it does say you can't do it and that will change a lot of people's behavior.

So I think that is an area where we can take a look at some of the problems that we're facing and we can tweak around area in order to increase some of the protections that are of concern. But I think I've...what I've observed generally is that we've got a framework that actually allows us to get some of the population level benefits that we need, speaking broadly.

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

Yeah. Great. And I've got Lucia in the queue and I'm going to put myself back in the queue, too. So, Lucia?

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

Yeah, thank you. I have this question primarily for Anna and I will Anna, I am a privacy lawyer and I've had doctors say, oh no, you can't have that information about your children, so, I feel your pain acutely. I think every privacy lawyer who takes care of their families' healthcare has had somebody say something like that to them. I guess I was wondering, in your experience as a patient, have there been things where it actually worked were you could get the information you needed without people's misunderstandings of the current rules being something you had to struggle through? Any good news there that we can say, oh, that worked, let's try to make that happen more often? Oh, I hope there's some good news there.

Anna McCollister-Slipp – Co-Founder – Galileo Analytics

Well, I mean admittedly there are a lot of reasons why I can't get access my data, I mean, and whether it's the CGM company wanting to protect their intellectual property around algorithms or whatever, I mean, it's not just privacy and that's just one that's very difficult to refute, because it seems to me, as a non-expert, that it just uses this blanket excuse, in part because the process is so opaque that most patients can't really articulately argue against it.

In terms of good news, I mean, I have noticed that my doctors seem to be a bit more free in e-mailing me recently, which is helpful. Most of them will use their private e-mail accounts which makes me suggest that their health institutions are watching who they e-mail and what they e-mail to patients, but often times that's the only way that I can actually get my lab results, because I can't get them online through the lab company or God knows what help HealthVault is supposed to be populated with. But, I mean, that has been really helpful.

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

And so, let me just follow up on the lab. So, since the new clear regs come out, and I'm getting really technical, let's just say in the last 12 months have you literally gone to a lab where you had your blood work done and said, can I have my results and you can't get them or...?

Anna McCollister-Slipp – Co-Founder – Galileo Analytics

Oh yeah, oh yeah.

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

Okay, depressing, but thank you for being honest.

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

And, as a follow-up question to that, this is Stan; Anna, have you found that they won't give you them at all or they won't give you an electronic format that's usable or all of the above?

Anna McCollister-Slipp – Co-Founder – Galileo Analytics

They will mail them to me.

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

Right. So my question was a little bit follow-up to what Lucia had as well. And we've talked some about use categories and the reference I think was either Rich or Steve might have said, there are some uses that are always okay, maybe that's...opt out. There are some uses that are never okay, you know, the discriminatory or denial uses. And others where maybe there is a role for control by data subjects and as I hear you talk Anna and I hear Mark talk about civil rights, it seems like that's a framework that is still starting to hold in some ways, that if the use by the data subject, which is your control, your ability to either pull it out or allow others to access it, is a model that you like, but then there would be other uses where there just simply not going to be appropriate for use. I mean, is that a framework that you've thought anything about, this panel?

Anna McCollister-Slipp – Co-Founder – Galileo Analytics

Well, this is Anna; I mean, from my perspective, I mean once the data has been de-identified, I don't really think that I or anybody else really has the right to restrict it being used. I mean, and I know that a lot of patient advocates disagree with me and I respect their disagreement, but from my perspective anybody who is getting healthcare today has benefited very directly from lots of sacrifices from other patients who participated in clinical trials or clinical research or just from the knowledge, a cumulative knowledge of physician care and clinical care. And I feel like that I do not have the right, once privacy is protected and de-identification is achieved and I'm intrigued by the notion of sort of criminalizing re-identification, once that privacy has been achieved, I don't feel like I have the right to keep other people from accessing my data to be able to learn things that would help improve the care of others.

It's just a way of doing things more efficiently, it's the same thing we've done over the years, we're just doing it far more efficiently in a more democratize way. I think what's critical is that every data point that's in an EMR system or that's "owned by" a data aggregator or an insurance company, begins with an individual patient who may have known, but probably did not know that they would be contributing data that would ultimately become a financial resource or an advantage to a company or an individual, and, that's dog. And I feel like there needs to be a commitment to social responsibility to make that data available to researchers, I don't want it personally, but to make it available to researchers or others who are serving the needs of patients, so that they have a better understanding.

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

Anna, were you're talking about de-identified or identifiable data in that comment.

Anna McCollister-Slipp – Co-Founder – Galileo Analytics

De-identified.

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

Okay. Mark or Michelle, do you have thoughts on that as well?

Michelle De Mooy – Deputy Director, Consumer Privacy Project – Center for Democracy and Technology

The only, I would agree with that actually, de-identified data is, for the most part, should be able to be used. But of course the rub is that a lot of what we presume to be de-identified can be re-identified and that's been sort of proven time and time again. I still think de-identification is a really important tool, but I think there also needs to be research and anonymization, and I know that there is, but I think supporting that is crucial; making sure that governments and other systems, state governments and municipalities, understand how to de-identify and are aware of sort of best practices and good examples of it. I think that that's sort of the low-level, but really important piece of the puzzle, too.

Anna McCollister-Slipp – Co-Founder – Galileo Analytics

I think that the key to being able to do it and making people trust what you are doing is that there needs to be transparency about what is being accessed and why. I've participated in, as somebody who's sort of a comparative effectiveness research geek, I've participated in a number of different forums or seminars, and one of the concerns is, is this insurance...if my insurance company can access this data to make decisions that will make it easier for them to exclude me from access to a particular drug?

Well, if they can access the data, then I would want the American Diabetes Association or the Kidney Foundation to be able to access the same data set so that they would be able to say, well, that policy doesn't make any sense because we looked at the same data that you have and this is what we've found. So there needs to be transparency both in methods and access so that there's a counterbalance, so there's a watchdog capability that the larger healthcare community has the ability to do by accessing the same data set.

And again, I emphasize that every data point that every insurance company or data aggregator has begins with an individual who probably didn't realize that they were contributing that. So I don't have a problem with people selling it and making money from that that gives them an incentive to normalize and clean the data, that's totally fine, I support that. But I do think that there's a responsibility that thus far I have not seen to give that data back to the community in the form of making it available to researchers.

Mark Savage, JD – Director of Health IT Policy & Programs – National Partnership for Women & Families

This is Mark. The one thing I would add to what's already been said harkens back to the recent conference on big data and civil rights which is, there was actually a lot of discussion about de-identified data and whether it was truly de-identified or could be re-identified. People did like the notion of a prohibition on re-identification, but even with that, there was still a discussion about harm to individuals and harm to communities. So some of the examples that I listed about where you could use greater demographic granularity to reduce health disparities or to increase the risk of profiling, those are harms that can go beyond the individual and can be experienced at a community level.

So I'm saying this because I think the current framework may do a lot. if we have some of the prohibitions, may do a lot at the individual level; I still think there's thinking to be done, as this conference was trying to do that thinking, about making sure that there are not harms at the population level or the community level. I don't have the answers there; I just want to flag the point.

Michelle De Mooy – Deputy Director, Consumer Privacy Project – Center for Democracy and Technology

Yeah, actually Mark, I think one of...this is Michelle, one of the interesting things I've been think about lately with regard to that is the use of services like 23andMe, which I think is coming up soon and the fact that as an individual, when you...if you choose not to posit your data or do anything, get your DNA...get your genetic profile basically, but family members do, then you're sort of providing that information against your will, or maybe that's too strong, but basically that information about you is out there. So I think that's an important frame for some of what happens in health data, that there are consequences individually, but sometimes the consequences extend to a population without an individual's express permission. And that's certainly a place where I think that some sound policies can be drawn, some lines can be drawn.

And the other thing, it's kind of worrying, but I just wanted to say, the collection of the information is something that's crucial, why do entities have this information? And I think with health data in particular, that question needs to be enforced, you know, why are you collecting this? Do you need to hold onto this? Because so many times commercial entities will collect data and then just hold on to it for some future use, which is unnamed, because they think it will be valuable. And that has to stop, particularly when it comes to sensitive data.

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

Deven, I see your hand up still.

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

Yeah, so I wanted to probe on a particular type of big data analytics, maybe it's not just one particular type, but the ability to, and I think Michelle, it goes a little bit to your point about collection limitations, which I know you guys have done a lot of work on. So one of the values that often gets noted with big data and is the idea that we don't...not only do we not have all the answers, but sometimes we don't have the questions, right? And that you can take big data sets and allow sometimes some of the information that is promising and worth further exploration essentially percolates from the data itself, right? So rather than bring the questions to the data you are letting, in some ways, the data surface the question.

And in that case, it's been argued that a collection limitation could suppress the idea that amassing data and letting it talk to you a bit, can sometimes be incredibly revealing and while not necessarily by itself revealing definitive causal information or even definitive correlations, it often will lead you to take subsequent pathways that can help you address other important questions, when you can be more specific and therefore bring the questions to the data. So interested both in your thoughts on that as well as the other panelists in terms of how you address what is a customary collection limitation Fair Information Practice against the idea that a lot of innovation comes from letting the data do the talking.

Michelle De Mooy – Deputy Director, Consumer Privacy Project – Center for Democracy and Technology

Yeah, and I think that that makes sense. I don't know if this is where you were getting with that but I think that de-identification is sort of one of the answers there, right? I mean, I think that you don't need to identify data necessarily, you don't need personal characteristics or personal identifying name, address, etcetera to be attached to it to let it talk to you, I think. You may need certain parts of that, but probably not all of it.

So I think it's really getting down to sort of one of the other principles, the data quality and making sure that you're drilling down into what pieces are a part of a certain framework of a puzzle, maybe you don't have the questions but you certainly have an intention. And so I think whether or not, a business could say, well we don't know yet, and I think that's unacceptable when it comes to health data. I think there needs to be a requirement to draw some frame around the collection of the data and the use of the data and allowing for some of that innovation to happen as long it's de-identified.

Anna McCollister-Slipp – Co-Founder – Galileo Analytics

Yeah, from my perspective...this is Anna. From my perspective once it's been de-identified I don't, I mean, I think we would be remiss in not keeping longitudinal data and storing it for quite some time. And in fact, that's precisely what my company's platform is designed to do, is to allow you to be able to follow your intellectual curiosity and to generate new hypotheses and then validate them. So, I'm a huge fan of that process and think that that's ultimately what we need to do more of is to let...allow researchers and clinicians to be able to explore and play with the data and let the data tell them things that may be important that they never thought were important. But it does need to be de-identified, I mean, I think that's absolutely critical.

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

Thank you.

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

This is Stan and Anna, I don't want to get into too technical of a conversation, but when you say de-identification is critical is there a level...are you talking regulatory de-identified or are you talking more anonymized, removed...identifiers like the Common Rule or what's your general perspective?

Anna McCollister-Slipp – Co-Founder – Galileo Analytics

Well, I mean, I don't really know, I'm just speaking very generally, I'm not an expert on de-identification.

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

Yeah, and I didn't mean to try and make you one. The reason that I brought it up is I think it's a hugely important area and I think we're going to get into it on our next panel. And it's hard to talk the same language across this concept and have everybody shaking their heads yes. In the prior panel, Rich Platt was talking about certain circumstances where we had to have identifiable data. So, I mean, I do think that I'm looking forward to that topic in the next panel as well.

Anna McCollister-Slipp – Co-Founder – Galileo Analytics

Right. Well the people in the next panel will be far more expert than I could even pretend to be at a cocktail party.

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

Well, we've got a couple more minutes if any other additional questions or thoughts for the panelists?

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

Stan, this is Lucia, can I ask a question?

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

Of course.

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

So, I don't know if this is the right panel, but we have a couple other lawyers on here and something that I've really been kicking around in my head is, as I've listened to both of the first two groupings today, is we all have a pretty easy time recognizing somebody doing something bad on purpose, discrimination on purpose with sort of malintent or because they're mean. And I think part of what we don't know is how do we prevent our analytic needs from resulting in a discriminatory impact that maybe nobody intended to cause. And I know that from that 50-year history of civil rights litigation, it's pretty hard in court to get all of that sorted out. And I was wondering particularly for Mark and Michelle, do you have any insights about, you know, don't go there if you're trying to solve for this problem with big data or look in this direction if you're trying to solve this problem for big data of sort of inadvertent impact discrimination?

Michelle De Mooy – Deputy Director, Consumer Privacy Project – Center for Democracy and Technology

Hmm, I'm thinking, it's a good question.

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

And honestly, as we set up and we teed this up and kicked it off, we don't know all the answers and you don't have to know all the answers, too. And if the answer is, well, that's a good question and we need to explore that more, that is perfectly okay because it is a really hard question.

Michelle De Mooy – Deputy Director, Consumer Privacy Project – Center for Democracy and Technology

That's a good question that we need to explore more. No, but I do think that there has actually been quite a bit of exploring, which is great, on de-identification and I think it's so difficult, right, to put a frame over what is a harm, like we talked about in the very beginning for one person or one community versus another. And I think that some of, like I said before, some of the sort of factors are starting to rise to the surface because of these questions.

For example, who is creating the decision-making mechanisms? Not, you know, not something we probably would have asked, but because of this sort of conversation about what makes...what impacts the population, how do we inadvertently do that or create harm is looking at the mechanisms that are making the decisions for us and then who's designing them?

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

I think we have David McCallie, I think we'll let you take us out, the last question here.

Mark Savage, JD – Director of Health IT Policy & Programs – National Partnership for Women & Families

Could I add something before we get to the last question? This is Mark.

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

Sure, Mark.

Mark Savage, JD – Director of Health IT Policy & Programs – National Partnership for Women & Families

The one thought I'd have to add is that if we go back to the Fair Information Practice Principles and this is more conceptual but I think there's something important here. There is...the collection limitation, the purpose specification; the uses could go a long way towards helping prevent that kind of problem from happening. I don't think that they are applied nearly as well as they could, but they're a good framework to start from and I think applied both at the individual level, which is the way they're tailored at the collection of the information from the person, but maybe something...a framework like that more broadly at the big data level.

Anna McCollister-Slipp – Co-Founder – Galileo Analytics

Could I just say...?

Michelle De Mooy – Deputy Director, Consumer Privacy Project – Center for Democracy and Technology

And actually, just one further thought, just really quick. I think there's also...there could be some exploration of when a, just begin about a commercial entity for example, veers towards diagnostics type stuff, right, where the FDA sort of came out for example against 23andMe. But for this...in the realm of health data, diagnostic or analysis, that's when I think you start to tread into an area where there can be harm and there can be inadvertent impact. So that might be one way...one sort of area that could use some further discussion.

Anna McCollister-Slipp – Co-Founder – Galileo Analytics

This is Anna and I think that these are really important points but I will say as sort of a counter to that that right now, the data that we're using to make decisions is not at all representative. We know that minorities don't participate in clinical trials at the same level as non-minorities and whether you're talking about different ethnicities or you're talking about smaller patient, more specialized patient cohorts, we're using data from randomized control trials of populations that don't really look like a lot of people who are impacted by the policy decisions that are made based on it. So we have to come up with a better way of doing it. I'm not saying that we don't need to think very clearly and consider these matters, but we need to start with where we are and right now we're making decisions based on very inadequate data.

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

Okay. So process question for you, Deven. Do you think we could go one more, let David round us out if we have time.

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

Yeah, yup.

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

Okay, David?

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

Thanks. So it's a broad question and we've touched on it a lot, but I'll just ask maybe from a different perspective and that is, in some cases the best we can do is to try to mitigate the harms that could occur from abuse...from unintended consequences of data. So in most recent politically interesting example is the Obamacare prohibition against denying insurance due to pre-existing conditions where data that could have harmed you in the past is now, at least to some degree, not so harmful.

So my question is in the context of big data, what are the best opportunities to think about mitigating of harms? Are there approaches to mitigate some of these unintended consequences, assuming that the data gets out somehow?

Anna McCollister-Slipp – Co-Founder – Galileo Analytics

I am glad that you mentioned the Affordable Care Act prohibition of exclusion of chronic conditions because I think that's absolutely critical and I think that a lot of concerns about privacy up until and still including now, are based on the fact that insurance companies have chosen to discriminate on individuals based on their health data. So hopefully that will stay in effect, pending the Supreme Court decision, but that is a huge hurdle for being able to effectively use big data.

In terms of other safeguards, I mean I couldn't possibly try to predict what the potential harms might be, I think that those will come and evolve as we get more and more sophisticated and we get further down the road. But I think that critical to understanding them will be a complete transparency, whether it's of algorithms or access to the data and knowing who has access to it and having some degree of understanding of what their purpose is. I think that's going to be the best...sunlight of the best disinfectant and if we understand who is accessing it and why and what they're doing with and other people have the ability to do counter analyses using the same data set that may contradict a policy, whether it's a private company or a government policy decision, then that will be the best way to counterbalance any prospective harm.

Michelle De Mooy – Deputy Director, Consumer Privacy Project – Center for Democracy and Technology

I would also say that I think the FTC and other agencies have a role to play in helping us as sort of a community to figure out what are some of the boundaries and what are some of the ways in which harm occurs? And I think some of their narrow cases have been helpful, they have a fairly broad application of fairness and deception and I think those are actually pretty useful in the way that they apply them to different cases. And they've started doing more in health and privacy and deception in terms of what's promised and what actually happens with data and I think that those can be instructive.

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

Great. Okay, thank you very much a panel and we're at time. So point of order, we have our next panel scheduled to start at 3:45 PM, do we have time to take the full 10 minutes or do we want to keep it to the 3:45 PM time?

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

Let's try, you know, we're...let's see if we can give people 5 minutes...

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

Okay.

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

...to take care of what needs to be taken care of and get right back.

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

Let's stay on the 3:45 PM start with the next panel, then and we'll talk to you all then.

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

Thanks, Stan.

Michelle De Mooy – Deputy Director, Consumer Privacy Project – Center for Democracy and Technology

Thanks, Stan.

Anna McCollister-Slipp – Co-Founder – Galileo Analytics

Thank you.

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

Okay, 3:45 PM. That went fast, 5 minutes.

Fred H. Cate, JD - Distinguished Professor and C. Ben Dutton Professor of Law - Indiana University Maurer School of Law; Director of the Indiana University Center for Applied Cybersecurity Research and Center for Law, Ethics and Applied Research in Health Information

Hello.

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

Hello, it's Deven; can you hear me?

Fred H. Cate, JD – Distinguished Professor and C. Ben Dutton Professor of Law – Indiana University Maurer School of Law; Director of the Indiana University Center for Applied Cybersecurity Research and Center for Law, Ethics and Applied Research in Health Information

Hey, Deven, it's Fred.

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

Hi, Fred, how are you?

Fred H. Cate, JD – Distinguished Professor and C. Ben Dutton Professor of Law – Indiana University Maurer School of Law; Director of the Indiana University Center for Applied Cybersecurity Research and Center for Law, Ethics and Applied Research in Health Information

I'm fine, thank you.

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

Great, we were just on a break; I'm just trying to get everyone back on. Khaled, are you on and ready?

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

Yes, I am. Hi, Deven.

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

Hi. How about Bob Gellman, are you on?

Robert Gellman, JD – Privacy and Information Policy Consultant

I'm here.

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

Okay. Terrific. Then we'll go ahead and get back into this with our third panel. Our first panelist is Khaled El Emam, who is the founder and CEO of Privacy Analytics, among many other things. We're very much...you might have heard, I don't know Khaled if you were on for the earlier presentation, but we...the issue of de-identification did come up, so you're pretty well teed up for your presentation and we look forward to it. You have slides, right?

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

No I don't.

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

You don't; that's fine.

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

I sent a write up, my commentary in the documents.

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

Yes, which we have, but I just wanted to make sure that we weren't missing anything. So go ahead and get started.

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

Okay, great. Well thank you very much for giving me the opportunity to present these points. So, I have six points and most of them focus specifically on de-identification/re-identification. So I'll start off by talking about re-identification attacks. So there has been a narrative around re-identification attacks that I believe is somewhat misleading and represents a misinterpretation of the existing data.

We did a systematic review of the evidence on re-identification attacks, focusing on health data a couple of years ago. What we basically found was that what you would expect, that if you de-identify data properly and use some of the existing known methods to de-identify data, that the success rate is very low for attacks. But if you don't use existing methods or don't de-identify your data at all and that data is attacked, then the success rate of these attacks is high, which is an obvious statement. But the fact remains that most attacks on health data, most re-identification attacks on health data were done on data sets that were either not de-identified at all or not properly de-identified.

So de-identification is one of the most powerful privacy protective tools. The narrative around de-identification networking is just inconsistent with the evidence; it's a good story to tell, but is just inconsistent with the evidence and if you want to make evidence-based decisions, you really have to be careful and nuanced about how we have these conversations. There was an article that appeared in a BioMed Central journal recently on the sharing of public health data and they made the point very nicely about how discussions about anonymization and data de-identification or how this narrative around de-identification is causing organizations not to share their data, which is really where we don't want to be. So there's a need to have a better informed conversation, an evidence-based conversation about re-identification risks.

So the next thing I'll talk about is de-identification standards. There are good de-identification methods and practices that are in use today. They take into account of realistic threat models; they take into account factors such as, what are the contractual controls, what's included in the contracts and what are the security and privacy practices that exist at the data recipient site. In fact, there's a lot of innovation that is happening on de-identification methods, but there are no standards which means that there is no heterogeneity in how de-identification is actually done.

So in order to raise the bar in terms of de-identification practices and to build a large community of practice around de-identification of health data and to encourage the adoption of de-identification, you really need to have standards. And these can be...they can be different standards, general standards, those for clinical trials, those for...special data, those for claims data or EMR data...effort and they need to involvement of industry, professional associations and academia. But I think that should we develop standards, I think we should, I think that will help tremendously with improving practices and developing this community of practice and have more experts available to de-identify data.

Then the third point that was in the kind of set of questions that were provided earlier was around regulatory changes. So I think that the de-identification methods and the HIPAA Privacy Rule, they're quite prescriptive and they've been in use for close to 10 years now, so there's a lot of experience applying them and we know what works well and what doesn't work well. There are two methods, as you know, the Safe Harbor method and expert determination method.

The only comment I would make about changes is that there's accumulating evidence that the Safe Harbor method has some important weaknesses and the kinds of weaknesses mean that under certain conditions, it will allow the sharing of data that has a higher risk of re-identification. So I think we need to have an evaluation of the value and the risks from keeping or continuing to use things like the Safe Harbor standard.

The Safe Harbor standard for de-identification is being copied and used by uncovered entities and is actually being used globally, it's been copied globally as well. So, we need to revisit the value and the risks from using such simple standards for de-identifying data and maybe additional guidance is needed to limit the situations under which such a simple standard...such a simple method should be used.

The fourth point is on stigmatizing analytics or creepy analytics or discriminatory analytics, but the basic idea here is, if you use data to make stigmatizing decisions is orthogonal to de-identification. You can make societally beneficial decisions from de-identified data or from identifiable data. So really these are two different concepts that should not be mixed together. So you can de-identify the data that gets, now let's talk about decisions you make from that data or the models that are built on that data.

There are really two ways to manage those, the uses of the data; you can modify the data algorithmically and in order to block inferences from the data. There are a bunch of techniques that have been proposed, they don't work very well, and that's why nobody uses them. The best way to manage this is through governance mechanisms because the decision of what is an acceptable use of the data is going to be subjective, it's culturally specific and it will change over time. So essentially the practical way, I think, to do this is, and we have applied, is to set some form of ethics committee or whatever you want to call it, data access committee, that will review the data uses within an organization and provide feedback to the business or to the analysts, but whether a particular data use would be stigmatizing, discriminatory or not. We can have a conversation about the composition of this committee.

The fifth point is around privacy architectures. So I'll just say something about safe havens, a lot of discussion about these, of safe havens for providing access to data. There are some advantages and disadvantages to save havens, which are covered in a bit more detail in my write up. But you still need to de-identify the data that goes in to Save Havens because the data still has a none/zero possibly not a very...not necessarily a very small risk of re-identification, even when you put it within the context of Safe Havens. So, these do not preclude the need to de-identify the data, although the extent of de-identification may be less.

And then the last point I want to talk about distributed computation. So there has been a lot of interest in applications of distributed computation and this really allows you to avoid pooling data and having to deal with all the data sharing issues around pooling data for multiple sources, so you push the computations out to the data sources and have the analysis done where the data is. A number of different...then are being used; you have secure computation protocols, you have meta-analytic approaches and then you have distributed queries.

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

Okay Khaled, I think we might have to let you detail those last two in the question period because we're...

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

Okay.

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

...holding people...

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

I'm over time?

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

Yeah, over time. Thank you, though, I'm sure we'll get back to those...

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

I'll stop there. Okay.

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

...because we have a lot of time for questions. Okay, so the next panelist...thank you...is Robert Gellman, who is a Privacy Information Policy Consultant here in Washington, DC.

Robert Gellman, JD – Privacy and Information Policy Consultant

Hi. I want to talk about big data, I'm not interested in the stuff that's de-identified because whether it is a de-identified or not is another issue, and of course Khaled talked about that. I want to talk about big data that is identifiable. And basically my problem at the beginning is, I don't know what big data is, you know, every year, every decade for the past couple of hundred years, we've have had more data and more analytics than we had in the past.

I've never seen a definition of big data that is precise and this is important because if you want to make a legislative or regulatory exception for big data, you have to define it with precision. And the problem is, once you do so, anyone can make all of their data big data by simply dumping in as much data as necessary to get over the threshold and exempt themselves from whatever privacy standard you have. So, I have a lot of trouble here; until I see a real definition, I just don't know what to make of the concept.

And I am concerned that some of the usual suspects who have always opposed privacy rules have jumped on the big data bandwagon to argue against privacy rules. This is essentially the same argument we've heard for a very long time that consumers, individuals have no privacy rights, that they have to prove harm in court, before they have any interest that makes any difference and the goal is anything goes. This is essentially what the marketers want to do. And this is what goes on at NSA; anyone who wants no restrictions on data collection will be certainly welcome at Fort Meade.

The other side...another side of this is that big data advocates make all kind of vague and unbelievable promises of things that will happen if we only have big data, you know, cancer will be cured, we'll all be rich, everyone will live forever; whatever promise they need to make in order to convince someone to loosen privacy rules, that's what they'll say. What we've got, what's still, I think, is the poster child for big data is Google Flu Trends, which didn't work, and by the way, didn't need identifiable data to do what it did. So basically where I come from is, I'm not prepared to trade my privacy cow, as it were, for a handful of magic beans labeled big data.

Let me turn for the minute to the health area specifically. I'm not sure I understand the need for any particular recognition of big data in the context of HIPAA. We already have a method for making patient records available for any kind of legitimate research. There's no reason to think that it needs to work differently for "big data" than for any other kind of data. And indeed if you said, for some reason, if you define big data and said, okay, the HIPAA restrictions don't apply to big data, the result would be perverse. If you would say to people who hold the data they could disclose it without process, without restriction, everybody would set their own rules.

Today we have a common set of rules under HIPAA; everybody goes through the rules and follows the same process. If there were no rules, we would have different procedures at every institution that held health records, and those who want the records would find it even harder to get records than they do now. Those are the points I wanted to make and I yield back the balance of my time.

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

Spoken just like someone who has justified plenty of times. Thank you, Bob, very, very helpful. Our next panelist is Fred Cate who is a Distinguished Professor, and C. Ben Dutton Professor of Law at the University of Indiana, Maurer School of Law. Fred, thank you for joining us today; we are ready when you are.

Fred H. Cate, JD – Distinguished Professor and C. Ben Dutton Professor of Law – Indiana University Maurer School of Law; Director of the Indiana University Center for Applied Cybersecurity Research and Center for Law, Ethics and Applied Research in Health Information

Great. Thank you very much Deven, I appreciate it. I will be brief both because I fear you and also because I am cowering in the corner of the hotel lobby.

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

Oh no.

Fred H. Cate, JD – Distinguished Professor and C. Ben Dutton Professor of Law – Indiana University Maurer School of Law; Director of the Indiana University Center for Applied Cybersecurity Research and Center for Law, Ethics and Applied Research in Health Information

Let me say first of all, I mean, I've been doing privacy for about 20 years and I usually think about it in a fairly dispassionate, research based way. I have to say, I feel especially invested in the health privacy issues because I've also been diabetic all of my life and I have lived a life in which healthcare was translated into numbers. You know, you live for the blood test results, for the blood glucose monitoring, I live with a pump and the idea of trying to transform that data into something that not only helps lead to better treatment for me, but also supports research and supports other secondary uses that may lead to advances that ultimately cure the disease, is pretty close to my heart.

And I should also add I led an NIH funded study on the issue of health privacy for which I am both grateful, but also can't help but reflect on that experience when thinking about the questions you posed. So, let me just make four fairly quick points. One is, today privacy laws in general seem sort of overly focused on individual control. And I say overly focused, I mean ever since Alan Weston first defined privacy of the interest of individuals in controlling information about themselves, Congress has picked this up, the Supreme Court has picked this up and it's reflected in many of our secondary documents and it's an inadequate definition of privacy. It's an inadequate aspiration.

But it's also, and this is my second point, it's an impossible expectation today to think that one's going to control his or her own data and to be frank, it's an undesirable expectation. It's one that as we've had extensive research, including the IOM Report in 2009 that showed, if we really allow that to happen, the effect is significant impediments to the availability of data for treatment, for research and for other valuable purposes. I might say, as part of the NIH grant I mentioned earlier, we did focus groups with the National Health Council, working with nine different groups of patients or patient caregivers and it was interesting in those settings, although the people conducting the groups spent extensive time talking about privacy, talking about the risk to privacy and so forth, these were not feelings that the patient and caregiver participants actually picked up on.

Their first and greatest concern is that information being used to try to address their condition, to make sure nobody else suffers from it. And they were struck to a person, without exception, when they heard that under HIPAA that couldn't take place unless you either had individual consent or IRB approval or complete de-identification, which researchers say in many cases makes the data hard to use for researcher, in some cases impossible, that they were really astonished by that. Interestingly, when asked what was their major concern about how a health care institution might misuse their data? The number one issue they raised is they did not want to be contacted. They didn't want to be contacted for consent, they didn't want to be contacted for marketing, and they didn't want to be contacted at all. So the third point is that it strikes me...

W

No, no, we did it...

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

I am sorry, who is this?

W

Yeah so...

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

Actually, can we not have interruptions to a person who is presenting please? Thank you. Go ahead Fred, I stopped your time.

W

Yeah, yeah, it was fine. So I opened the line for you and I at 10 and then everybody else joined at 10:30, so, it worked out fine.

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

I am sorry about this Fred, I'm not sure what's going on there, please continue.

W

I'm actually at a virtual hearing for...

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

Altatum, can you shut that line down? Oh, I know who it is, Donna, can you mute? So sorry, Fred.

Fred H. Cate, JD – Distinguished Professor and C. Ben Dutton Professor of Law – Indiana University Maurer School of Law; Director of the Indiana University Center for Applied Cybersecurity Research and Center for Law, Ethics and Applied Research in Health Information

No, the perfect example of why we don't allow individual control of information, instead we want systems to protect data. In other words, privacy is too critical of a value, it's too important to leave up to this notion that individuals should police themselves. But it's also a balance and that is the critical issue that seems to reflect in all of the modern research and that's how patients look at it, it's how caregivers look at it; it's a balance between privacy and also wanting the benefits that come from their data being freely available to be used in appropriate ways, and often that does mean with de-identification.

Now this is the final point, especially important as we see increasing demand for the data, increasing value of the data; whether you call it big data or not, I actually agree with Bob, which will probably make him want to change his view, but I don't think this is a big data issue at all; I think it's true of all data that we need to be thinking about how to make sure data is protected at the same time that it's available. We don't let the mechanisms of protection by themselves interfere with the responsible use of the data.

And I would just end with a really conclusion from the 2009 study from the IOM which found most that the HIPAA Privacy Rule does not protect privacy as well as it should and also that it impedes the use of data for important health research. And I think it's addressing both of those, that's one reason I'm delighted to be on the call today. Thank you.

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

Great. Thank you very much Fred, very appreciated and again, apologize for the interruption. I think we just had somebody who didn't realize they weren't muted. So, all right, so now we're moving into phase of questions and I'm going to, we don't have anybody teed up yet, so I'm going to take the moderator's prerogative to let Khaled provide a few more details on the last two points that you were trying to make during your time, which is the...I recall the idea of safe havens and sort of distributed computation or, I may not be framing it right. But you didn't have very much time to talk, particularly about the last one, so I'm going to give you some time now to talk about it.

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

Great, thank you, Deven. So, it was just one final point around distributed computation methods. So these various methods are in use today. The only caution I would make is that many of those don't have security evaluations or security proofs, actually have not been developed and we've written a number of analyses showing vulnerability to some of those systems. So, my only suggestion is that it's important to do security proofs and evaluate security protocols for these distributed computation systems, because some of them, some of the big ones actually in deployment today, may not be as secure as we think. Just because it looks like no data is being shared, there may be leaks in the intermediate results that are being shared in order to compute the final results of the analysis. So, proper security proofs are important. I'll leave it at that.

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

Great, thank you very much. David McCallie?

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

Yeah, okay, good. My question is for Khaled and I'll apologize that I am not enough of an expert in re-identification attack methodologies to ask the question in an appropriately formal and rigorous way. But I just will point out that it is a subject to considerable debate that there are folks who believe that it is, in fact more of a risk, the re-identification risks even of data that is identified with our best algorithms is still reasonably high. And just to register that that's an active debate in the re-identification community, as you know.

But specifically, just to ask you, it seems to me that the biggest risks come when there is some way to join the data, mesh the data with other data that exists completely outside of the control of the de-identification step. And I was wondering if you could comment on that in this, so-called era of big data when there is so much more behavioral data available about us that the incredibly high dimensional space that results makes it pretty easy with just a few data points to identify unique paths through that data space when you can join it to someone else....join it to these external data sets. And so does your confidence in our de-identification technologies, is it based on the assumption that those joins are impossible or do you think that even if those joins are done, it can still be de-identified?

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

So, just to get to your first point about the debate; look, everybody can have an opinion, but let's look at the evidence. And the evidence doesn't support the statement that even properly de-identified data can be successfully attacked, right? So if you want to be evidence-based, you'll draw a conclusion, but certainly there is a debate and many people have opinions.

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

Yeah, I mean, a little bit of it comes down to math though, right? I mean statistics and math, the arguments, the good arguments are not based on an attempt, and they're based on actually looking at the dimensionality of the spaces. So...but keep going, I...

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

Okay.

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

It's hard to go do that experiment because there's not a lot of data that people are willing to put up for a test.

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

So actually, so just this touches on your second point. If the data is de-identified properly, then the issue of dimensionality is taken into account. And the empirical...the evidence is important because it's really hard to do those attacks, because when you share, you often times you stipulate additional controls on that data, I mean, you'd have contractual controls, you would have controls in terms of how the data is secured, how...so you have security and privacy controls imposed on the data recipients and so on. And this is how you're going to be able to share rich data sets and in those contracts, you can prohibit the joining of data sets, you can prohibit re-identification attempts and so on. So, it's not just the modifications to the data, it's all the controls that you would apply on the data sharing.

And if the de-identification is done well, then that joining would be very hard as well, the success rate would be small, which acts as a strong disincentive for doing the joining anyway, if the de-identification is done properly. Public data is a little bit of a challenge in order to protect against these types of...this type of meshing and joining than the amount of de-identification would have to be significant. But for non-public data sets or quasi-public data sets, you can do a pretty good job to get good quality data by modifying the data a little bit and then imposing all these additional controls. And so this is well-established approach for managing the risks when sharing data, and also to ensure high quality data comes out at the other end.

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

So, this is David again; just to then to echo what I think I heard you say is that it's a combination of the controls put on the uses of the data plus the de-identification technique applied to the data.

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

Yes, that's the standard way, practical way of sharing data, includes modification to the data as well as a series of controls and the intensity of the controls are balanced with the amount of data de-identification you'd apply to the data.

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

Okay and I would say I agree with that point, that point makes a lot of sense to me. And the risk is then associated with somebody who is capable or willing to break those controls and re-identify the data for nefarious purposes. But we can take that debate to some other setting, but you clarified the point and I appreciate the clear answer. Thank you.

Robert Gellman, JD – Privacy and Information Policy Consultant

Can I weigh in on this?

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

Yeah, of course.

Robert Gellman, JD – Privacy and Information Policy Consultant

Two quick points; one is, and I leave the real debate about how de-identified something is to some of the statistical experts, but I will make a political point that all you have to do is take supposedly de-identified data and use whatever techniques you want and identify a senator's wife and the world will blow up, you know; so the studies are all very nice, but I don't find them politically convincing.

My second point has to do with the controls where I very much agree with what everybody said and I just wanted to point out, I've written a law journal article on this topic, it was in a Fordham Law Journal a couple of years ago, you can find it if you look, where I suggested a legislative framework, it could be a regulatory one under HIPAA if you worked at it, whereby you allow data to pass back and forth to people, you have administrative controls, you have contractual controls, you have legal controls and you have a variety of enforcement methods under the statute I proposed; all of which lead in the same direction of keeping data from being re-identified and holding people accountable if it is.

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

Yeah Bob, we'll...I'll make that article avail...this is Deven; I'll make the article available to the workgroup.

Robert Gellman, JD – Privacy and Information Policy Consultant

Good.

W

I was going to ask that, thank you Deven.

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

So Lucia, you're next.

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

Oh perfect. I had two questions; I think they're both really short for Khaled. One is, I just want to clarify, when you talk about safe havens, could you, for me not the technologist, tell me is that the same as other people call an enclave or are those two different things? And if so, what is each? And the second one is, could you, is it appropriate in this setting for you to identify some of the weaknesses with the Safe Harbor rule that you think have come to light since it was enacted, however, 10-12 years ago?

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

Okay, yes. So the term safe haven is sometimes also enclaves is used, virtual data laboratories, research data centers; all of these mean variants of the same thing, but essentially you create a closed environment where data users can come in and access the data either remotely or they have to come physically on site in order to access the data. They can't pull the data out; they can't take the data out with them or download the data.

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

Okay.

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

So, and there are different ways to do this physically or through a VPN or some form of remote access.

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

We have terminology issues sometimes in these debates and I wanted to make sure we were all talking about the same thing, so that's helpful, thank you.

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

And then with respect to Safe Harbor, I mean, there are a number of different things. The analysis that would make Safe Harbor a good method makes some assumptions and if you meet those assumptions then it's protective, but if you don't meet the assumptions, then it may provide very little protection.

So for example, one of the assumptions is that dates and zip codes are two indirect...the only two indirect identifiers that can potentially identify individuals, but it ignores other information like race, ethnicity, language spoken at home, number of children, visit dates, rare diagnoses; so if you have any of these other pieces of information in the data, they will contribute to re-identification. But they are completely ignored by Safe Harbor. If you don't...

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

Okay, so they're left in, at the end of the day, they're left in in the Safe Harbor and they can sort of build...we were talking earlier about a mosaic effect, I don't know if you were on then, but it sort of helps that process of refilling back in the empty spaces and the data that de-identification would normally generate.

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

Right, so if you have...yes. So under Safe Harbor data said you can have all that information in the data, which means that the risk can high, under the expert determination method, you would deal with that information, you'd evaluate whether the information is increasing the risk and if it is, then you would generalize it or do some other manipulations to it.

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

Okay, that's helpful. Thank you.

Fred H. Cate, JD – Distinguished Professor and C. Ben Dutton Professor of Law – Indiana University Maurer School of Law; Director of the Indiana University Center for Applied Cybersecurity Research and Center for Law, Ethics and Applied Research in Health Information

Could I add a comment on the expert method?

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

Yes.

Robert Gellman, JD – Privacy and Information Policy Consultant

The expert method, if you have a proper expert is fine. However, there's no transparency to it, we don't know what methodologies are used to make the assessment. So you can go off, and the word I'm going to use here is hired gun, you can go find someone who will claim to be an expert and say whatever you want to hear. There's no oversight of that, there's no way to find out what's going on. I think the expert method is fine, but it need...what the Rule, as written now, needs a lot more substance to it, a lot more process, and a lot more procedure before it can really be accepted.

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

Hey Deven, this is Lucia. Can I ask Bob a follow up question about that?

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

Yeah, yeah, yeah.

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

So, would that be alleviated by, I don't know, a lot of professionals have licensing standards or some kind of standards so that you know that they meet minimum qualifications. Is that really sort of the implication of what you're saying, maybe some way of saying people who are allowed to do this are all cap...all meet these criteria?

Robert Gellman, JD – Privacy and Information Policy Consultant

Maybe, I'd really rather have Khaled answer that question, because he knows the field better than I do, but I'm thinking in terms of maybe if you're an expert, you have to publish something about what the method is that you use and so other people can look at it.

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

Okay.

Robert Gellman, JD – Privacy and Information Policy Consultant

And I think in one forum I once suggested the idea that experts should publish their methodology and you could hire...you could have graduate students go look at them, just for fun and see if they can poke holes in them and see if the methodology is good. This could be a nice homework assignment for someone in an advanced statistical course, and that would be one way of providing some kind of oversight of what's going on.

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

Can I add a comment to that?

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

Yeah.

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

So I totally agree with Bob, I think that when we ta...just to define standards for de-identification and this will serve multiple purposes. It will ensure that the methods that are being used are known, are published, are scrutinized and then the certification of individuals, I think, would be fantastic if we can get there. So you have standards then you need to have a body of knowledge, you'd have exams and certification schemes around that, then that will increase also the pool of experts.

One of the challenges that exist today, I mean I just said the Safe Harbor has weaknesses. If you go to the expert determination method, there is not a large pool of experts; we need to grow that pool of experts. And so standards, certification schemes will help with creating this community of practice around de-identification and will make it a lot easier to implement more sophisticated de-identification methods and practice.

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

So you mean that the 12-year-old study statistics, right?

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

Sorry...

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

I'm making a joke, it's okay. I'm just making a joke about how do we get more experts; you have to know statistics to do this, right, so...

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

Well, I mean, I don't think that the level expertise needed can be packaged.

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

Okay.

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

So, there may be very efficient ways to do with...by packaging the expertise through automation, so it does not necessarily have to be 12 years of practice.

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

Thanks.

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

So I actually have a follow-up question on the Safe Harbor point that you've made Khaled. When I looked at, I know we've talked about this in the past about Safe Harbor having some weaknesses and so in some ways it's not surprising that it would, over time, grow either weaker or less certain in its conclusion that there's very low risk of re-identification because it is static; 18 categories of information that might have worked very well back when the regulations were first promulgated, but doesn't necessarily stand the test of time and we've never reevaluated it.

Having said that, one of the things that was somewhat persuasive to me in looking back at the rationale for having a Safe Harbor was to have something that was very easy for people to use. So that they wouldn't have to hire additional help and that they could deploy a de-identification methodology and therefore have a very strong incentive to go in that direction because it wouldn't be hard for them to do, they...you know, anybody...a caveman could do it, right, to borrow from the commercial, because 18 very clear categories. So what do you think of those arguments? And is there any rationale for a cookbook methodology at all anymore or have we just really gone past that?

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

Well, this is a very good argument for something that is simple. But I think that by developing standards around expert determination method, you can come up with something that is still somewhat simple and that is, if it's well packaged, that it can be broadly applicable and then we can move away from the weaker approaches. So the objective is a very good one and it's a very important one, but I think we need to rather than maintain the weaker methods, we should try to make the better methods more accessible and much easier to adopt; again standards, certification and training, better packaging and so on.

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

Hey Deven, this is Lucia. I have one more follow up question about that, because I don't know if Khaled listened to our earlier session, but in our first session we were sort of talking about the potential usefulness of a never do this, always do that kind of set of bookends on how you should be handling the data. And it seems like that's consistent with what I'm hearing you say, which is there are definitely some sort of, it's not a bad idea to have something a caveman could do, but we might need to change what the recipe is in this particular case.

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

Exactly, yes.

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

Okay, thanks.

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

Okay.

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

After even all of this time has passed, I think we can do a much better job and still make it accessible.

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

Yes.

Robert Gellman, JD – Privacy and Information Policy Consultant

Let me broaden this question in a different direction, I mean, I agree with what everyone has said, but it's tempting to say, oh well, if we're going to give out data that's de-identified according to the formula but let's be safe and let's have a data use agreement with it. That's...there's some attraction to that; however, the other side of this is, I'm a doctor say, and I want to give a lecture and I want to say, I treated a bus driver with cancer. If we don't have some kind of recognition that some of this data can be discussed in public in some ways without creating any kind of a privacy concern, I mean that's what you get from this de-identification method that limited information can be made public. Whereas making all of the 18, you know, making the larger quantities of data public, I don't...you know, is more problematic. I don't know if there is some way to deal with the what can we make public thing without going to this 18-element kind of thing.

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

Right.

Robert Gellman, JD – Privacy and Information Policy Consultant

I don't have an answer to that, but I pose the question in the hopes that maybe somebody else does.

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

Right, that's relevant to the data needs to provide information, right Bob, it's not just data.

Robert Gellman, JD – Privacy and Information Policy Consultant

Right.

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

But if the presentation about the bus driver or the truck driver identifies that individual, then that's not good either.

Robert Gellman, JD – Privacy and Information Policy Consultant

No, no, I agree with that, but the only things you make public is, I treated a bus driver with cancer; that's not...that by itself with no other data, doesn't identify anybody.

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

Right.

Robert Gellman, JD – Privacy and Information Policy Consultant

So there is a co...we have to allow the medical profession and researchers to talk about some things in public, we can't make everything...

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

Right.

Robert Gellman, JD – Privacy and Information Policy Consultant

...totally restricted and that's sort of the other side, here.

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

Yup.

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

David, you're up.

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

Yeah, so I'll change the direction away from de-identification back to, Fred Cate, your statement that I translated in my notes here, everybody wants the benefits; nobody wants the harms, which is your point about the balance between the potential benefits and the potential harms of using big data or small data or any data. What my question is the same question I asked a previous group which is, if there are one or two things that you could go address on the harm side, what would that be? In other words, are there approaches that we could take through revisions of our current laws or regulations that would address some of the harms that might shift that balance towards making us more comfortable with the use of data about ourselves?

Fred H. Cate, JD – Distinguished Professor and C. Ben Dutton Professor of Law – Indiana University Maurer School of Law; Director of the Indiana University Center for Applied Cybersecurity Research and Center for Law, Ethics and Applied Research in Health Information

Well, I mean, I appreciate the question. I think one thing, and frankly listening to Khaled talk, makes...reinforces this is, the way in which the identification is largely addressed in HIPAA is very much a technological one or, if you will, a process one. And I think the idea of, as the Federal Trade Commission has recommended, strengthening the idea of legal requirements that attach to that as well so that data shared under a de-identification would be subject to limits on even the effort to re-identify it. And that then might allow one to work with less de-identification, in other words, for example when we talked with patient groups about what do you consider to be de-identified, their concern was not, could somebody reverse engineer it with a supercomputer; it was, if the data were blowing down the street would their name be on it with their Social Security nu...would be immediately highly visibly identifiable.

And so it seems if we need to be working towards ways that would say for some things we may want complete, as complete a de-identification as we can get. But it seems like for many others that may not matter; especially if we could combine it with strong legal requirements that would attach automatically that would limit re-identification or attach criminal or civil penalties to re-identification. That seems like that would make a much more complete package. I mean, I think the way you characterized it is completely accurate, which people want the benefits and they don't want the harms.

I think as a practical matter though, what people who sort of study or research in this area worry about is, we don't want the tools creating additional harms. And so it's hard enough having to balance risks and benefits, but we don't want the privacy protections themselves creating new opportunities for mischief and so if nothing else, we should try to clarify and in many ways to tighten those so that we have clearer protections, but then also that make clear what you can do towards, say for example, medical research, without making it, as currently the case, where if you ask five different institutions, you'll get five different answers.

Robert Gellman, JD – Privacy and Information Policy Consultant

Could I weigh in on this a little bit?

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

Yes.

Robert Gellman, JD – Privacy and Information Policy Consultant

I agree with a fair amount of what Fred said, but I think the question in a way focuses on the wrong thing, I don't like to see the debate here talking about harms. This is rights; people have rights with respect to their data. They're not absolute rights; there are other concerns that have to be considered and weighed, but people have rights whether they're harmed or not and as far as I'm concerned, if you have my data, if you collect data about me and that collection, that compilation of data is a harm. And if you give it to somebody else, I am harmed thereby; it may not be a direct immediate visible harm, but I am placed at greater risk as a result of the compilation and maintenance of data about me by anybody.

Fred H. Cate, JD – Distinguished Professor and C. Ben Dutton Professor of Law – Indiana University Maurer School of Law; Director of the Indiana University Center for Applied Cybersecurity Research and Center for Law, Ethics and Applied Research in Health Information

Right and just to be clear, I obviously would disagree. In other words, rights...you can assert rights, but there's no legal basis for those rights. The only legal rights we would recognize in data would be against certain uses by the government. We might very well want to say that there should be some additional rights, and maybe we should have legislation to create those, but as a practical matter I guarantee you the public would disagree with that. The public would say, if you can use my data in a way that does not cause me risk of harm in terms of I could lose my job, I could lose my insurance, that...and you think you could do something that might make treating my condition better, they would support it to a person.

Robert Gellman, JD – Privacy and Information Policy Consultant

I disagree, there are a whole series of polls that show people want to be asked for consent before their records are made available for medical research and I actually disagree with that. I think that's the wrong answer, I think we need in other methods like IRBs or something to make decisions on behalf of people, at least in the current environment, but people want to be asked for consent.

Fred H. Cate, JD – Distinguished Professor and C. Ben Dutton Professor of Law – Indiana University Maurer School of Law; Director of the Indiana University Center for Applied Cybersecurity Research and Center for Law, Ethics and Applied Research in Health Information

Let me just say again, I think you would find most of the modern data disagrees with that and we have the studies cited by the IOM, we have the Lindstrom studies, we have the studies the National Health Council did; they all show that people want some ultimate right to opt down, but they do not want to be asked and they do not want the research to depend on waiting for them to answer.

Robert Gellman, JD – Privacy and Information Policy Consultant

Well, if you guys care, you're going to have to find your own facts on that.

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

We are happy to collect data on...that's relevant to the points that you both made. It's always helpful, and actually I'm glad to be having this debate because Linda Kloss is really up next. I was about to ask a question about sort of what is the role of consent? And actually based on Bob's answers, I think you can...notwithstanding some disagreement about what people do and don't want, it sounds like you both may be closer to agreement at least on some points than in conflict. But I...since I have already asked a lot of questions, I'm going to pause on that one, come back to it and go ahead and defer to Linda, because she hasn't had a chance yet.

Linda Kloss, RHIA, CAE, FAHIMA – President – Kloss Strategic Advisors, Ltd.

Well, if you want to continue that, along that line, that's fine. I actually was going to go back to de-identification, so...

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

Oh, okay.

Linda Kloss, RHIA, CAE, FAHIMA – President – Kloss Strategic Advisors, Ltd.

...maybe it's wise to go forward and then just let me circle back.

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

Okay, yeah, because we do have time. So, all right, so on that question, it sounded to me from the discussion that the two of you were having that while you were disagreeing about sort of what people want, based on what's been measured in survey data and through other instruments, but it also sounded like you both may have been saying something about the role of consent for uses of data in research and I want to tease that out a little bit more. Fred, I'll start with you and then Bob and then you can go back and forth for some period of time until we have time for Linda to ask her question.

Fred H. Cate, JD – Distinguish Professor and C. Ben Dutton Professor of Law – Indiana University Maurer School of Law; Director of the Indiana University Center for Applied Cybersecurity Research and Center for Law, Ethics and Applied Research in Health Information

Or until somebody interrupts us; I actually think consent has a very useful role but I think you have to focus it to where there are meaningful things to consent to. So the idea of saying, we have this long privacy policy, you haven't read it, but would you sign this form saying you've read it, that strikes me as meaningless consent and a complete waste of time. And to be perfectly honest, it discredits the whole idea that we're all about of trying to protect privacy or make data available for productive uses.

And so I would focus consent either as a safety valve, like as an opt out, as we do in many other settings where you'd say, look, if you really object to this, we're going to make it possible for you to express that but we're not going to make the whole enterprise wait while you think about it or why somebody tries to present opportunities for you to consent, for example, while you're signing your insurance forms or while you're signing your admission forms. And then I would really focus consent on things that we think people might care about.

And it is interesting, I mean, one of the things that shows up in a lot of the focus groups is, for example, the place where we do have opt out today for directory information, that's actually something many people do care about, they want to say, if I don't want people to know what hospital room I'm in or if I don't want them to know general information about my condition, I want to be able to say that. So maybe that's a place maybe where we really do focus consent. Interestingly, all of the survey data, and that's a...Bob and I would not disagree on this, shows that people want to consent over many of the things that we do not let them consent over today, like sharing data with the government, for example. But what I would not do is use consent as a, we don't know what to do so let's throw in a consent requirement.

Robert Gellman, JD – Privacy and Information Policy Consultant

Well I agree with a lot of what Fred said. I think that as a society we can make a decision and this is a decision we've made for years that somebody can basically consent on your behalf, the IRB, that society has an interest in health records and it's perfectly fine if you have a legitimate process. And whether the IRB process is good or not is a whole separate subject, but that's what we've got. And if society can make that decision and say for the greater good, everybody's record's going to be used with protections and all that sort of thing. On the other hand...I agree with that, full stop.

On the other hand, we have a lot of new technology here, you know, everybody's talking about electronic health records and people involved in their health care. All of a sudden we have mechanisms that enable us to actually ask people, we can find them, we can economically ask them for consent, we can do things that were impossible to do in the past. And I think that some recognition of that needs to be given and there needs to be more thought. I still don't think that...I basically agree with Fred's sort of opt out thing.

I think there are other ways of doing things, for example, if I have a rare disease I should be able to put a note in my health file that says, I agree to any study that the national organization of rare diseases thinks is worthwhile or, I agree with the Catholic Church's policy on health research, or I agree with the ACLU standard or somebody else. There are a lot of creative ways of using technology, but at the end of the day, at least for some kinds of research, there's still the right of society expressed through law, regulation, what have you, to say, we want to...we're going to opt for the greater good here and we're not necessarily going to give you the chance to consent.

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

That's incredibly helpful, thanks to both of you. Okay, Linda, you can steer us back to de-identification, at least for now. We still do have plenty of time to continue on either topic, so.

Linda Kloss, RHIA, CAE, FAHIMA – President – Kloss Strategic Advisors, Ltd.

Yeah, wonderful dialogue; I would like to go back to the discussion...the recommendation around the need for de-identification standards and probe a little bit more on the level of those standards and how you envision that. What has been attempted? Where are we with that? And then Khaled, your thoughts on balancing moving towards standards for de-identification with your comment that there is now currently a lot of innovation in this area and how do we preserve that innovation while moving to a more rigorous set of standards?

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

So, in terms of the standards making efforts, I mean there are some general health data related standards, so there is...the HTRUST Alliance is working on a standard that they had announced that effort I think about a year ago and that work is progressing. So that's an industry, essentially an industry group and that's a general health standard for de-identification. I don't know when it will deliver, but the expectation is in the near future.

And then there are some standardization efforts that are specific to clinical trials data; so there are a number of clinical trials transparency initiatives happening in the industry, driven by the European Medicine, well, I shouldn't say driven, catalyzed by the European Medicines Agency, policies around data sharing. So, there are a number of professional associations that are working on clinical trials data sharing standards and these are expected to deliver in the first quarter or early second quarter of next year. So we'll see what these look like.

There are various other industry efforts to develop standards, mostly around clinical research and clinical trials, but they haven't gone public yet. But again they are expected to have something sometime next year. So I think in the first half of next year, we'll start seeing things come out with respect to standards for sharing different types of health data.

In terms of how these would work, I think having the standards being data specific makes sense; clinical trials...standards for sharing clinical trials data are going to be different than standards for sharing geospatial data that's used in public health, for example or just generic health data standards. So splitting it up that way makes sense, but they have to be operational because what people want to do is put in place a scalable process for sharing data so that it can be automated, so that it can be packaged, so that people can be trained, some people can be certified, so that that whole process can be scaled.

Right now we have a scalability problem with de-identification and if the standards are not designed to facilitate scaling, then we may not progress very much. So if we're able to scale de-identification, then we'll essentially have more data available and share it in a responsible way. So that's...I don't know if that answers your question.

Linda Kloss, RHIA, CAE, FAHIMA – President – Kloss Strategic Advisors, Ltd.

It does, I think like so much in our health information ecosystem, sometimes we end up with too many sets of standards and confound, so I think that this is an area that might bear some additional dialogue.

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

The other comment I will make is that I see a lot of demand for standards because a lot of organizations that want to share data are looking for guidance and the lack of concrete detailed guidance is inhibiting or slowing down their willingness to share their data. And I see that quite frequently actually, so, I think it may help make more health data available for research and other secondary purposes.

Fred H. Cate, JD – Distinguished Professor and C. Ben Dutton Professor of Law – Indiana University Maurer School of Law; Director of the Indiana University Center for Applied Cybersecurity Research and Center for Law, Ethics and Applied Research in Health Information

This is Fred; can I just add, I think that's true across the board in this area. In other words, even liquid IRBs, one of the things we find is IRBs desperately wanting some guidance and feeling that it's pretty far out of their comfort area to start evaluating privacy issues, especially when they get conflicting advice or they get no advice. And the idea of trying to provide clearer standards rather than sort of what the Privacy Rule does now, would be one way to try to again, irrespective of what the outcome of the decision is, at least make the decision process not itself become an impediment to their responsible use of data.

Linda Kloss, RHIA, CAE, FAHIMA – President – Kloss Strategic Advisors, Ltd.

We...this is Linda again, and I think we should also probably be cognizant in all of the new users for this data; communities are starting to use the data for local community health projects and with very few resources. And I think a high need for some agreed-upon standards.

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

Is that just an...so Linda, this is Deven, is that just in the area of sort of de-identification or does it take on a broader dimension, what I think I heard in Fred's comment which is, how do you evaluate sort of what is the privacy risk or the risk to privacy interests of this data subject, you know, for any type of research where...that involves reuse of data? Is it, so, when you say...when you're talking about needs for standards, it almost sounds to me like we're talking about that the guidance is both on the techniques for disclosure control or minimizing re-identification risks of data, but also about a whole spectrum of, you know, how do you evaluate the risk of data in terms of approving a research use of data and strategies for mitigating that risk that are beyond just de-identification and just consent.

Linda Kloss, RHIA, CAE, FAHIMA – President – Kloss Strategic Advisors, Ltd.

The whole range, yes.

Fred H. Cate, JD – Distinguished Professor and C. Ben Dutton Professor of Law – Indiana University Maurer School of Law; Director of the Indiana University Center for Applied Cybersecurity Research and Center for Law, Ethics and Applied Research in Health Information

This is Fred, again. I think that's the perfect example, in other words, if you could move to a set of even some, I don't know what you call them, standards or norms, so that you have in place these protections and you're talking about this type of data and you're using it for this purpose. Then there would be some presumption around that use that if it met those requirements it would be acceptable. It would be minimal risk, it would be high benefit and it would be whatever you want to call it and that part of the problem is we treat every decision today as if it's...we just start over and say, what now? And so that's why particularly in multi-center trials, literally, I mean it's no exaggeration, if there are 10 IRBs involved, you will get 10 separate positions and that's not protecting anything, that's not making good use of data and it's certainly not protecting privacy.

Robert Gellman, JD – Privacy and Information Policy Consultant

Could I just add a point on a slightly different direction here?

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

Of course.

Robert Gellman, JD – Privacy and Information Policy Consultant

Just something that I think everyone on this call, everyone who's listening already knows there is tons of health data that's not protected by HIPAA...

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

Right.

Robert Gellman, JD – Privacy and Information Policy Consultant

...and that's going to increase over time and that just makes all the problems harder.

Fred H. Cate, JD – Distinguished Professor and C. Ben Dutton Professor of Law – Indiana University Maurer School of Law; Director of the Indiana University Center for Applied Cybersecurity Research and Center for Law, Ethics and Applied Research in Health Information

Well, and just to echo Bob's point, with which I agree entirely and I think frankly it's the elephant in the room. In other words, I would argue that a great portion, maybe a majority of the data that's going to be relevant to both health treatment and health research is not currently covered by HIPAA. And to be honest, because of the various confusions around HIPAA, companies are going out of their way to keep it from being covered by HIPAA. And so that means, as a practical matter, again privacy is not being protected and yet the data aren't being made available for valuable uses like research.

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

I see that. So, I'm looking at my queue, I don't have anyone in it; if somebody wants to jump in or verbally put themselves in the line, please do. I have in my mind cued up a transparency question, we are reaching closure but we're not quite there yet. All right, since nobody jumped in I'm going to ask it.

So on some of our prior panels, some of our panelists were recommending doing a lot more to be transparent to the public, to data subjects about data uses and this would apply not just to uses of identifiable data, but to de-identified data. Now Dr. Rich Platt in an earlier panel said, it would be hard to necessarily tell individuals what their particular data were used for and nor could you necessarily do that in detail, but to do a better job than we currently do of being upfront with people about actual data uses. And it's still not an easy thing to do, I think, have any of the three of you given thought to that or do you want to provide some input on that? Because it was a theme that was in some of our earlier panels and it hasn't really come up in this one.

Robert Gellman, JD – Privacy and Information Policy Consultant

Well, I think there should be more transparency on research activities and on IRB's and that when protocols that are sent to IRBs for approval, probably should be made public and those that are approved probably should be made public. I don't expect individuals to read these, but other folks may and if someone's doing something that's over whatever someone thinks is the line that's allowable it will get attention and there will be a response to it. And I think that kind of thing is useful and will actually build public trust.

Fred H. Cate, JD – Distinguished Professor and C. Ben Dutton Professor of Law – Indiana University Maurer School of Law; Director of the Indiana University Center for Applied Cybersecurity Research and Center for Law, Ethics and Applied Research in Health Information

Yeah, this is Fred; I completely agree with that. And I think one of the real problems we've had in US law is confusing notice with transparency. And the problem is notices get so technical and because of the way they're enforced, they get so vague that we end up with notices nobody reads and nobody understands if they do read and we achieve no transparency out of them. And in a way, we would be better, whatever we do about notices, to say look transparency is achieved through other means and that means the information may have to be more broad, it may have to be more general, but it's also going to be more informative as opposed to, you know, 65 screens of a privacy notice.

And I think that would offer significant advantages. One of the things that certainly the emphasis on our NIH work really stressed is the ethical importance of transparency, particularly if we're saying to people, your data may be used without your explicit consent or this could be a higher public interest that controls here that increases the ethical need for transparency in broad or general terms around pieces of the data and the benefits and risk that creates.

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

Great, thank you very much. Well I'm...we're a little bit ahead of schedule but it's also the end of the day. Do the panelists have any additional points that they want to make before we move to our public comment period? Okay, well thanks to all three of you for making the time and we really, really appreciate it. We'll take all of your points under consideration and as I had mentioned earlier today, we will be processing what we learned here today through many, many workgroup discussions, which continue to be held in the public. We may, in fact, come back to you with additional questions as we go along and we appreciate any additional input that you have on those. But for now, thank you so much for sharing so generously of your time.

Fred H. Cate, JD – Distinguished Professor and C. Ben Dutton Professor of Law – Indiana University Maurer School of Law; Director of the Indiana University Center for Applied Cybersecurity Research and Center for Law, Ethics and Applied Research in Health Information

Thank you.

Robert Gellman, JD – Privacy and Information Policy Consultant

You're welcome.

Khaled El Emam, PhD – Canada Research Chair in Electronic Health Information – University of Ottawa; Associate Professor, Faculty of Medicine - University of Ottawa; Founder and Chief Executive Officer – Privacy Analytics, Inc.

You're welcome.

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

And now we'll...Michelle, I think that you can take us into the public comment period.

Public Comment

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

Thanks Devin. Operator can you please open the lines?

Caitlin Collins – Junior Project Manager – Altarum Institute

If you are listening via your computer speakers you may dial 1-877-705-6006 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

It looks like we have no public comment.

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

Might be one advantage to having a 4-hour meeting is that we’ve pretty much exhausted everyone. Well thanks to all of you and good weekend to all and we’ll get back to this on Monday.

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

Thanks Devin and thank you everyone, we’ll talk to you on Monday.

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

Thanks all.

Public Comment Received During the Meeting

1. Should the HIPAA protections be demanded of companies that hold personal health data?
2. Regarding De-Identification, one needs to mention the OCR Standards, the OCR's two options to de-identify PHI. The comment, above, regards De-Identification Methods, as prescribed by OCR.

Meeting Attendance				
Name	12/08/14	12/05/14	11/24/14	11/10/14
Adrienne Ficchi				
Bakul Patel				
Cora Tung Han	X	X		
David Kotz			X	X
David McCallie, Jr.	X	X	X	X
Deb Bass	X			
Deven McGraw	X	X	X	X
Donna Cryer	X	X	X	X
Gayle B. Harrell		X	X	X
Gilad Kuperman	X			X
Gwynne L. Jenkins				
Helen Caton-Peters	X	X		X
John Wilbanks				
Kathryn Marchesini	X	X	X	X
Kitt Winter	X	X	X	X

Kristen Anderson	X	X	X	X
Linda Kloss	X	X	X	X
Linda Sanches	X	X	X	X
Manuj Lal				
Mark Sugrue				X
Micky Tripathi		X	X	
Stanley Crosley	X	X	X	X
Stephania Griffin		X		
Taha A. Kass-Hout		X	X	
Total Attendees	13	15	13	14