

HIT Policy Committee Transcript September 18, 2009

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director

Thank you. Good morning, everybody. And welcome to the fifth meeting of the HIT Policy Committee. Just a reminder, this is a federal advisory committee. It's being conducted in public. There will be minutes from the committee meeting in a week or ten days or so. A reminder to members of the committee to please identify yourselves as you speak, so people listening on the telephone and over the Web know who is speaking. And let me just have the panel, the committee go around the room and introduce yourselves very briefly. I'll begin with Scott White.

Scott White – Local 1199 – Assistant Director & Technology Project Director

Good morning, everyone. Scott White, 1199, SEIU.

Mike Klag - Johns Hopkins Bloomberg School of Public Health

Hello. I'm Mike Klag with Johns Hopkins Bloomberg School of Public Health.

David Lansky - Pacific Business Group on Health - President & CEO

David Lansky, Pacific Business Group on Health.

Judy Faulkner - Epic Systems - Founder

Judy Faulkner, Epic.

Gayle Harrell - Florida - Former State Legislator

Gayle Harrell, former state representative from Florida.

Rick Chapman - Kindred Healthcare - Chief Administrative Officer/CIO/EVP

Good morning. Rick Chapman from Kindred Healthcare.

Christine Bechtel - National Partnership for Women & Families - VP

Christine Bechtel, National Partnership for Women & Families.

Paul Tang - Palo Alto Medical Foundation - VP & CMIO

Paul Tang, Palo Alto Medical Foundation.

David Blumenthal - Department of HHS - National Coordinator for Health IT

David Blumenthal, National Coordinator.

Neil Calman - Institute for Family Health - President & Cofounder

Neil Calman with the Institute for Family Health.

Paul Egerman - eScripton - CEO

Paul Egerman, software entrepreneur.

Art Davidson - Public Health Informatics at Denver Public Health - Director

Art Davidson, Denver Public Health.

David Bates – Brigham and Women's Hospital – Chief, Dir. Internal Medicine

David Bates, Brigham and Women's Hospital and Partners Healthcare.

Marc Probst - Intermountain Healthcare - CIO

Marc Probst with Intermountain Healthcare.

Jim Borland - SSA - Special Advisor for Health IT, Office of the Commissioner

Jim Borland, Social Security Administration.

Michael Weiner - Defense Health Information Management System - CMO

Michael Weiner, Department of Defense Healthcare.

Frank Nemic - Gastroenterology Associates - Gastroenterologist

Frank Nemic, Gastroenterologist.

Judy Sparrow - Office of the National Coordinator - Executive Director

Thank you, and we do have any committee members on the telephone? All right. With that, I'll turn it over to Dr. Blumenthal.

David Blumenthal - Department of HHS - National Coordinator for Health IT

Thank you, Judy. Thanks to all our members and to the members of the public who are with us. We have an exciting day ahead of us. Some terrific presentations on a topic of great interest to the committee, to the office of the national coordinator, and I think to the public as well, and that's the issue of privacy and security of personal health information, stored and transmitted electronically, exchanged electronically in a health information system that is powered and enabled by electronic technology.

We are focusing today primarily on privacy. We will touch on the issues of security, but I'd say if there was a focus among those two related issues, it would be on privacy for today. I want to thank members of a taskforce that represented the health information technology policy committee in putting this day's work together. And members of the taskforce represented both the policy committee and our standards committee, and included Paul Tang, my co-chair, Deven McGraw, Latanya Sweeny, Paul Egerman, Dixie Baker, and Steve Findlay, as well as those are members of the policy and standards committee. And from the office of the national coordinator, Jodi Daniel, Suniti Ponkshe, Steve Posnak, John Ishee, Sue McAndrew, and Judy Sparrow. Sue was actually from the Office of Civil Rights, which has major authority under legislation for new authorities that are available for privacy protection.

We are here in a learning mode. We understand the importance of this issue. We understand that HITECH legislation increases the public's concern and interest. We understand that we have to get this issue as close to right as humanly possible in order for the benefits of electronic technologies to be realized in the practice of medicine and in healthcare generally.

After we hear the testimony that we'll hear today, we'll also go on to study the recommendations that were made by the health information technology standards committee just a few days ago on standards related to privacy and security. And those recommendations were made to me, as the national coordinator. They are only recommendations. They are not, by any means, etched in stone, but we pay close attention to our standards committee, just as we will pay close attention to the testimony we'll hear today and to the public input that will follow, and to the comments that we receive constantly from interested observers and members of the public.

There will be summaries. There will be reviews of today's testimony and of the standards. We then likely will do further work, probably both within the context of this policy committee, as well as within the context of the standards committee. I know the standards committee is planning further work on the privacy and security standards that they themselves recommended to us earlier this week.

This hearing is well timed because of those recent recommendations for standards. I wish we could say that we planned this hearing with foreknowledge that our standards committee would make

recommendations this week, but we're just lucky that the timing worked out the way it did. But I think it is auspicious that we have this first set of recommendations on an issue that we're about to deal with today.

We also are going to be thinking about, as we go forward, other issues and other agenda items for this committee. We've done an enormous amount of work, and I continue to be extraordinarily grateful to all the members who are here, as well as those who couldn't make it today for their commitment of time and intellectual effort and their fairness and objectivity and public spiritedness in serving the needs of the public through this process. But we have come to a kind of – after five meetings, we have accomplished a great deal, and I think, perhaps in our next meeting, we will discuss with you, some of us in the office of the national coordinator, will sit back and consult among ourselves and with members of the committee about a next set of issues that we might want to take on within the mandate that this committee has, which is a very, very broad mandate for providing advice to the national coordinator.

One area, for example, that we may want to think more about in the future is the Nationwide Health Information Network and how that Nationwide Health Information Network should be organized and governed going forward. The office of the national coordinator is actually specifically tasked with developing governance mechanisms for the Nationwide Health Information Network, and it's likely that we will be engaged in the very near future in rulemaking on that topic, and it's obviously a vital topic for the future of information exchange in this country.

We're also going to be working to coordinate our agenda with the national committee on vital and health statistics. They've done pioneering work for many decades in the field of privacy and security, and we'll hear from them today, one of their members today on their work, but they continue to be a resource to the federal government on the issues of data use and privacy and data exchange, and we want to coordinate our agendas going forward.

Having said that, what I'm going to do right now is ask Paul, my co-chair, Paul Tang, to go over specifically the agenda for the day, and then we will dive in. We are going to probably have a shorter break than is listed on the calendar today, but I will let Paul justify that to you and duck.

Paul Tang - Palo Alto Medical Foundation - VP & CMIO

What else is the vice chair for? Thanks, David. I think we all remember from the very first meeting, the first hour, we all agreed that and acknowledged that privacy is absolutely foundational to any initiative that would involve the storage, the access, or the exchange of confidential health information, and that we created privacy as one of the foundational categories in our meaningful use criteria. As David mentioned, we also have additional, sometimes named the ARRA 8, topics upon which this committee is supposed to make recommendations on, so it's fitting that our first full committee hearing deal with this foundational topic of privacy.

And so this is an informational hearing. There may be other kinds of ways we get information to go through and make some deliberations and potentially make some recommendations to the national coordinator in the future. But we'll deal with a number of hot privacy issues that we need to address as a country if we're going to wire the country and expect to safely transmit confidential health information to the authorized people who have a need to know.

David also mentioned that in the Recovery Act itself, there are a number of new provisions on top of the HIPAA that we know and love so well. And so Jodi Daniel is going to summarize some of these new provisions so that we're all on the same page, and to set a context for the hearing, as we go forward this morning. Jodi?

Jodi Daniel - Office of Policy and Research, Office of the National Coordinator

Good morning, everyone. It's very exciting to be here to have a hearing on privacy and security and health IT, and I'm excited to be able to kick this off. When we were setting this up, the taskforce that helped organize this thought it would be helpful, since everybody on the committee and potentially everybody who is listening might not have all of the background on privacy and security policies, and

privacy and security laws, and the changes that came out in ARRA, to give a little bit of a background for context for the rest of the discussion today. So that's what I'm intending to do.

Just from the onset, as you've heard both David and Paul say, the success of health IT and exchange rests on consumer and provider confidence in the privacy and security protections of the information. This is critical and fundamental to our achieving meaningful use of health information technology. And one of the ways that we're hoping to be able to do this is try to leverage the technology to improve protections on the existing policies that we have today.

But looking first at some of the existing policies that we have today, ARRA really builds on a foundation that has already been in place and is something that we're looking to build on top of that foundation, new policies to help advance our health IT and health information exchange efforts, so we have federal privacy laws, HIPAA privacy and security rules being the most prominent, but there are other federal laws on privacy of information, particularly health information, including rules regarding substance abuse treatment information.

But HIPAA really sets a floor for privacy protections and allows state laws to exceed those protections, so there's a whole host of state privacy laws all across the country that provide additional privacy protections on top of the federal protections that exist. It also represents some challenges for folks in trying to comply and understand all those varying state laws, and it's something that we've been looking at and working through at ONC.

There's also quite a lot of guidance on privacy and security, both in explaining how folks can comply with the HIPAA rules, but also last year, December of last year, we came out with a nationwide privacy and security framework for health information exchange that establishes sort of the backbone of our thinking of how privacy and security policies and practices should take place. This framework establishes eight high level principals for privacy and security, and it's something that we hope to build on this year.

We did use those principals as the basis for setting up the panels and the discussion we're having today to make sure that we're representing the whole array of privacy and security issues that are raised when we're talking about health information technology. And then we have a lot of policy development efforts that have been ongoing, most notably the health information security and privacy collaboration, which has engaged actors within 42 states and territories to look at their privacy and security policies in their state, think about how they work as we're moving to a more electronic role for the healthcare industry, and how that affects, how those state policies affect interstate exchange.

Then there's ARRA, and ARRA sort of changed this foundation and changed the game, and I'm going to spend most of my time talking about some of those changes. One of the most notable changes, I think, is the changes with regard to business associates. The Recovery Act has made it so that the HIPAA privacy and security – certain HIPAA privacy and security requirements now apply to business associates, and business associates can actually be held accountable by HHS for complying with those requirements. It also establishes that certain entities like health information exchanges do have to engage in business associate agreements with covered entities for exchanging of that information.

Another one that I think is one of the most notable changes is the new requirement for breach notification for health information. What this provision did was say that for covered entities and business associates, if there's a breach of health information that they have to notify patients of that breach. In certain cases, they have to notify HHS as well. OCR has recently come out with rules in this area, and I'll talk through that a little bit and what the status is of those rules after we get through the provisions.

What's interesting is that ARRA also went beyond just covered entities and business associates, and gave the Federal Trade Commission authority to require breach notification for vendors of PHR and other non-covered entities. So the FTC came out with a regulation as well that requires breach notification of those entities. And those two rules came out recently.

The interesting thing for both of these is that Congress in ARRA stated that if an entity renders protected health information unusable, unreadable, or indecipherable that the breach notification, there's no requirement to notify of a breach, so this is sort of like a Safe Harbor. If in fact you make it so the information is not usable to somebody who gets access to it and is not authorized to have access to it, then there's no requirement to notify in the case of a breach.

ONC worked closely with OCR in coming up with this guidance and basically stated that if information is either destroyed or appropriately encrypted that it meets this standard and, therefore, if in fact there's a breach, if the data, for example, is encrypted, the entity does not have to do the breach notification. So it's sort of pushing people to use heightened security measures with respect to their information so that they don't have to comply with those breach notification requirements. This is a Safe Harbor. It's not something that is a mandate, but it's something that is encouraged.

The Recovery Act also did a whole host of changes to the rules themselves and required guidance in a lot of areas. They provide now that the individual has a right to restrict disclosures a health plan for payment or healthcare operations if they pay out of pocket for that service. So if an individual doesn't want their health plan to know about a particular service that they receive, they could pay out of pocket, and then request and have that request honored that the covered entity does not share that information for payment or healthcare operations with the plan.

ARRA also required that a covered entity limit use disclosure and request for personal health information to limited data sets, so this is where certain types of data are stripped from the information, or if that's not possible, to use the minimum necessary, and required HHS to develop more guidance on minimum necessary to help covered entities in complying with that.

There are new provisions on accounting for disclosures. The accounting for disclosures provision under the HIPAA privacy rule requires that an individual can request information about disclosures made of their health information for particular types of disclosures, and usually these were the non-routine disclosures. What ARRA did was said now if an entity has an electronic health record, they would have to provide an accounting for disclosures for treatment payment and healthcare operations activities as well, those kinds of disclosures as well. This is an area where, as you'll see later, where they're looking for some guidance on standards, and where OCR will be coming up with some regulations.

ARRA also provides that a covered entity must provide an individual with a copy of their health information in electronic format if the covered entity has an electronic health record, and this committee, in making recommendations on meaningful use, does have recommendations about electronic access for consumers, so very much aligned with this requirement. There are a lot of these, a lot of changes.

The Recovery Act also prohibited covered entities and business associates from receiving remuneration for personal health information without the patient's authorization, and from receiving remuneration for using the information to make communications about products and services. There are some exceptions to these rules, but the goal here was to try to limit the ability for folks to use an individual's ... health information and receive compensation in exchange for that. The regulations also have – I mean, the statute also has some requirements for regulations to provide clear opt outs for covered entities in fundraising communications with individuals, so the individual has a clearer opportunity to opt out of any fundraising communications.

And this last one, I think, is really interesting and one that we're taking on at ONC is to do a study and provide recommendations to Congress on privacy and security requirements for non-covered entities, particularly PHR vendors and similar types of organizations. So PHR vendors and other consumer facing – vendors that provide consumer-facing tools may not always be covered by the HIPAA rules because they are providing a service to a consumer, not to a provider or health plan. In these cases, they may not be covered. And the question is, what are the right protections for those types of entities? How should the information be used or safeguarded when they're held by these types of entities? ONC is required to work with the Federal Trade Commission in thinking through some recommendations to Congress in this area.

One of the other key changes, I think, that affect the entire HIPAA privacy and security rules are the enforcement provisions in ARRA. ARRA extended the HIPAA civil and criminal penalties to business associates, so this is where there's sort of more accountability for business associates in complying with the federal laws. It also changed the civil penalty structure to increase the penalties and to give some more enforcement authority and teeth to the enforcement. In addition to that, not just relying on the federal government to enforce the HIPAA rules. Congress provided in ARRA that state attorneys general have authority to enforce the HIPAA provisions, and that's something that OCR is planning to provide some assistance to state attorneys general on how to do that.

Notably, there were some debates over the years about whether or not individuals or employees of a covered entity could be held criminally liable for violations of the HIPAA privacy rule, and some interpretations that they couldn't. So Congress came back and made a clear statement that in fact employees and individuals can be held criminally liable for violations of HIPAA under DoJ's authority to enforce the HIPAA rules. And, finally, under enforcement, ARRA required periodic audits by HHS to insure compliance with the privacy and security rules, and that's something that OCR is looking at right now on how best to do that.

Now, beyond all of the changes in the regulatory and the HIPAA privacy rules and the regulatory structure and the enforcement of those, there are a series of studies and reports that Congress had asked for in the area of privacy and security, in the areas of compliance with the HIPAA rules, to report on non-covered entities, and protections for those non-covered entities, as I mentioned. Report on best practices related to disclosures of health information for treatment purposes, which is something DAO is looking at, guidance on implementation for de-identification, and a study on the definition of psychotherapy notes. So there are some areas where there weren't specific changes in the rules, but there were requests by Congress for studies and for us to either provide guidance or provide reports back to Congress in some of these areas.

Finally, there was a focus on education, encouraging and requiring OCR to do some national outreach and education. This is something that they're planning to do with respect to HIPAA, and ONC has been working closely with OCR because we want to broaden the scope of that to provide privacy, educate, privacy and security education even more broadly than compliance with the HIPAA rules. OCR also is required to now have regional privacy advisors to help provide education in the regions for both providers and for consumers.

So now how is this all going to happen? I mentioned the breach notification regulations, and I'm just focusing here on HHS' regulations, noting that FTC also is regulating in the area of breach notification. HHS did a request for information in April 2009 on our guidance for how to render PHI unreadable, unusable, or indecipherable. We received about 80 comments on that guidance, and incorporated the comments into our final guidance, which went out into the interim final rule on breach notification that was published just last month by HHS.

It is an interim final rule, which means that it is final. It is effective September 23rd, so next week. According to the statute, it was 30 days after the interim final rule was published, but it is interim final rule, so what that means is we're accepting. HHS is accepting comments on this rule. The comment period ends October 23rd of 2009. And then HHS and OCR will be finalizing that rule to incorporate the comments that we receive.

There will be a separate regulation on enforcement just to explain some of the enforcement provisions that were put forth in ARRA. There were some areas where OCR wanted to make clear how the enforcement provisions work, although those are in effect currently. Those were one of the areas that became effective right away. Then, finally, there will be regulations on the HIPAA modifications themselves. All of the issues that I discussed that ARRA – where ARRA made some changes to what were in the HIPAA privacy and security rules, those will be incorporated into a regulation and the effective date for those modifications under the statute is February 2010, so OCR is working diligently on trying to come out with a proposed rule on those modifications.

Then you heard Paul Tang, and you've heard this committee talk about the ARRA 8 many times, and I thought it would be good to just put them up on the screen and make sure folks are aware of some of the – the ARRA 8 that apply to privacy and security, so I did cut some of them out, you'll notice, if you're familiar with the ARRA 8. And I also added in some of the optional ones, which go beyond the ARRA 8, so this is privacy and security topics that the health IT policy committee is supposed to take a look at according to ARRA.

The first is technologies that protect the privacy of health information and promote security in an electronic health record, and this includes the segmentation and protection. I have a typo there. Protection from disclosure of specific and sensitive individual identifiable health information with the goal of minimizing the reluctance of patients to seek care. This is the goal of trying to consider technologies for segmenting data so that patients and providers can choose to protect certain information separately from other health information. It also included use of and disclosure of limited data sets, so this is one of the ARRA 8.

There was another, and this was related, and I wanted to put it on here because privacy and security also goes to accuracy and integrity of data is infrastructure that allows for accurate exchange of information as another area that this committee is authorized and suggested to look at.

Technologies for an accounting for TPO disclosure – treatment, payment, and healthcare options disclosures – and I mentioned that was an area of change in the regulation that OCR will be making some modifications to the HIPAA rules on, and it's an area that this committee is expected to weigh in on.

Technologies that allow individual identifiable health information to be rendered unreadable, unusable, or indecipherable to unauthorized individuals, this ties into that breach notification provision. Just as a note, we are actually required by the statute to update that guidance annually, so as technology develops, as the ability to better secure information develops, the expectation is that we would modify that guidance to reflect the changes in the technology, so that's an area where your advice would be helpful.

And then, finally, and this is not in the ARRA 8, but this is one of the optional one's for you all to look at, is methods to facility security access to personal health information by an individual or person assisting in the care of that individual, so just a small task for the committee to take a look at.

Now I wanted to turn to standards, and David started talking about the standards committee and the privacy and security recommendations that the standards committee came out with, and so I wanted to just touch on those and put those on the folks radar screens and let folks know the areas for which those standards developed and some of the thinking that the privacy and security workgroup had in making those recommendations to the full committee and then the full committee making those recommendations to ONC.

The first thing I want to highlight before getting to the specific standards is that the standards that were recommended are standards for the products or platforms, but those are really enablers to protect information, and those standards don't necessarily protect the information themselves. They have to be part of a more comprehensive approach and tied to policies and practices for implementing those technologies and for implementing those polices. So we can have a standard for authentication of a user. Then we have to make sure that folks are actually using the technologies that are available, and that even if there are strong, say, password protections, that the practice isn't to post a sticky note on your computer that has the password on it and then averse all of the standards that we put in place in the first place.

So it really has to be part of a comprehensive approach for us to actually have good security in place. And what the standards committee did was suggest standards that should be and capabilities that should be incorporated into the technology. And they are planning to go back and look now at some best practices that folks should be considering and implementing those standards.

These are, as defined by the privacy and security workgroup of the standards committee, the domains and areas that they focused on. They had divided into product standards and infrastructure standards, and different domains and areas that they focused on. And I'm not going to go through. I will put my caveat. I am not a standards expert. I'm a lawyer and policy person, although I am here – I've gotten a great education on standards in the last few years, and understand enough, I think, that I can – that I know the significance and the policy implications of many of the standards that were recommended.

In deliberating on these standards, they were looking at a lot of different things. One, they were looking at making sure that they're architecture independent, so that they weren't dictating a particular architecture by selecting particular security standards. They also considered the maturity of the standards. They wanted to make sure that they were standards that were implementable, but they also wanted to think about how they're pushing the standards over time.

So they actually set up sort of a roadmap where they looked at 2011, 2013, 2015, for those security standards. And, in 2011, they picked standards to recommend to ONC that were mature and that were in widespread use. But then in 2013 and 2015, they picked standards that may be available, but not quite in widespread use, and expected those standards to develop over time to go along with the elevator that we talked about for meaningful use, getting people on the elevator. Trying to get them to start adopt, using the security standards, and then trying to move them up to using more and more secure standards over time.

A couple of ones that I just want to highlight, and a couple of other points I want to highlight – for privacy and security, the standards were recommendations for both inside the organization, as well as for exchange of information, which is different than the interoperability specifications, interoperability standards that the standards committee recommended. The interoperability standards were for exchange of information, but not necessarily for what an entity has to within their organization. In this area, the committee thought it was important that the standards apply both within the organization, as well as for exchange of information to make sure that there are true protections of the information.

They also made sure that when I mentioned that they were architecturally neutral, they wanted to make sure that they weren't stifling innovation by coming up with particular standards that sort of dictated particular architecture, and so that was something that was important in the transmission security standards and having an option for the standards that could be used in that area.

One area that they have noted that needs some work is the consent management standards. They did recommend standards in this area that sort of get the ball rolling and enable some level of consumer preferences, but it doesn't get to the segmentation of the data. There aren't standards in that area at this time, and there is some work being done, as I understand, from HL-7 and some discussions with HITSP in those areas. And the expectation is that as those standards develop, they would be looking at those and considering whether to make recommendations to us in those areas.

So another one that I just want to point out is the third one, accounting and audit. This one is tied very much to the accounting requirements that are in ARRA, and we are now looking with OCR at how those standards would work for implementing the accounting requirements that are in ARRA as OCR is looking at their regulatory process for incorporating those new accounting provisions into the HIPAA privacy rules, so that's my knowledge on standards. I'll defer to the standards experts on a little bit more detail in those areas.

I wanted to also just mention some input and guidance beyond ARRA that either we are working on or have been working on or are going to be working on that I think might help inform discussions here, and we're really hoping that or I'm really hoping that this committee and ONC can sort of work together in a somewhat iterative process so that we can bring issues that we're thinking about to you for consideration, have public input on some of the thinking that we're doing, and really have this be a public discussion on how we come to the right policies on privacy and security in these areas.

A couple of things that I just wanted to let you know about because I think they might be helpful to the committee is we have some reports on state laws in the areas of consent and access that are close to being ready for us to put out, and it provides a good basis for understanding the state law variation and where the existing law is today. There's a lot of confusion in that area, and I think these reports will be very helpful to help clarify some of that.

We have a couple of white papers that we're working on. We put a request for proposal on this, and we're close to getting going on this project, but I wanted to let folks know because this is an area where your input to us can be helpful, and where I hope the work that we're doing can be helpful to you all. So we are trying to get all of the – trying to get some thinking, comprehensive thinking on particular issues of priority all in one place. So what we're looking at is doing some white papers that are objective and that pull together all of the respective issues from various different perspectives and disciplines on a particular topic.

For example, the first two white papers that we're planning to do is one on consumer preferences and the second on segmentation. The goal here, so for instance on consumer preferences is, one, to get all the issues on the table, to understand the implications, for example, of whether doing opt in versus opt outs, and whether you mass data or not and what kind of implication that has to practice. You know, the input on how you collect consent or consumer preferences at the provider level versus the HIE level, any significance there. How much information and decision-making consumers will take on. Is there a point at which consumers will say this is too complicated and not take the responsibility? The human factors kind of issues, ethics issues, so trying to get all the issues in one place so that it can help inform our policy decision-making.

The reason I bring this to your attention is, one, because I think it can be helpful as discussion documents for those who may not be as familiar with all of these issues and all of the intricacies of some of these issues, as well as because, as you prioritize areas for consideration, we can then go forward and do similar white papers on the topics that you prioritize. We do have that built into our project. So hopefully, like I said, this can be a way where we can help provide support to you, and you can provide guidance to us on priority setting. Then we hope to do some further development on that nationwide privacy and security framework that I mentioned where we put out implementation guidance and best practices, and hopefully you can be informative to us in that area on how we can do that best.

Today's hearing, and you've heard David and Paul already talk a lot about this. A lot of effort went into planning this hearing. This is really our first entrée for this committee into privacy and security, and so we set this up to be fairly broad based to cover a whole lot of issues and to have this be a listening session so that the committee can then make some decisions and priority setting about where to go, what issues to take on, what more information we need, and how best to address those issues, either through existing workgroups or otherwise. So I really appreciate all of the effort of the folks who helped put this together, and they are planning to meet again after this meeting so that we can – to make recommendations back to the committee on how to proceed and some areas for priority setting and for taking on some issues, so I look forward to the discussion today, and I'd be happy to take any questions if folks have them.

David Blumenthal - Department of HHS - National Coordinator for Health IT

Any informational questions for Jodi? I'm sure there are many questions, but I also expect that hopefully some of them will get answered over the course of the day. Judy?

Judy Faulkner - Epic Systems - Founder

Is there any way we can get a copy of your slides?

Jodi Daniel - Office of Policy and Research, Office of the National Coordinator

Yes. I apologize for that. I didn't have them ready in time for folks to print them, but we'll make copies available to all the committee members.

David Blumenthal - Department of HHS - National Coordinator for Health IT

Yes?

Judy Faulkner - Epic Systems - Founder

One minor thing on your white papers – I think that’s an excellent idea, and I assume this committee will have some input perhaps on what various topics will be, or are they already predetermined?

Jodi Daniel - Office of Policy and Research, Office of the National Coordinator

No. We’ve predetermined the first two because we wanted to get them started, and they’re areas that we had either – consumer preferences was an area that we’ve heard about over many years. NCBHS had told us that they wanted us to take on the opt in and opt out discussion, so areas that we knew were priorities from either our own understanding or from other advisory committees, and then the segmentation we took on because it was something that was in ARRA that we thought actually, you know, there aren’t any standards in that area. We wanted to sort of think through those issues so we could help influence the standards development process. But at this point, we actually have not committed to other topics, and we do have funding available to do white papers in other areas, so that’s where I would look for input from this committee to help us prioritize what those topics should be, so there is room for input on those.

Judy Faulkner - Epic Systems - Founder

Terrific. I think the opt in, opt out is probably the most important one.

Jodi Daniel - Office of Policy and Research, Office of the National Coordinator

Yes.

Judy Faulkner - Epic Systems - Founder

I would hope that there’s going to be some focus groups or some additional study done on that topic before that white paper is actually produced. Are you going to be subcontracting those out, or is the department going to be doing that?

Jodi Daniel - Office of Policy and Research, Office of the National Coordinator

We’re actually contracting for the white papers to be done, so we don’t have that contract in place yet. We put out a request for proposal on that, and we’re still working through the contracting process.

Judy Faulkner - Epic Systems - Founder

Thank you.

Jodi Daniel - Office of Policy and Research, Office of the National Coordinator

You’re welcome. Yes?

David Blumenthal - Department of HHS - National Coordinator for Health IT

Jodi, I would like maybe some consideration given in regard to our future certification decisions we may have to make. Maybe a little more information in the form of the white papers on disclosure, and to the effect that they may or may not affect future systems capability or certification requirements that we want. Thank you.

Jodi Daniel - Office of Policy and Research, Office of the National Coordinator

All right. And I’m assuming that a lot more ... we don’t have to make commitments on these white papers today. I’m assuming that the debate and discussion today will help inform some of those priorities that the committee thinks are important for the committee to take on and for ONC to take on, so look forward to a future discussion on what those priorities should be and some road-mapping for privacy and security issues. Great. Thank you very much.

David Blumenthal - Department of HHS - National Coordinator for Health IT

Thank you, Jodi. It’s nice to see all that material in one place, if a little daunting. So what the task force has done is set up a series of panels. And, in each case, we’ve asked a committee member to play the role of moderator. But it’s going to be, I think, moderator light. I’m just trying to keep folks on time. But

what I'd like to do is introduce the moderator for our first panel, and that's Paul Egerman, and let him invite the panelists to come up and begin the presentations.

Paul Egerman - eScription - CEO

Thank you very much. Will the panelists come up to the table? The first panel is called patient choice, control, and segmentation of health information.

Paul Tang - Palo Alto Medical Foundation - VP & CMIO

Paul, if I can give just an overview of the whole hearing. We have four panels on four different sorts of major topic areas, and each of which could take a day in themselves, so we gave them five minutes, and I'll explain that in just a little bit. Basically we wanted to try to provide a breadth of perspectives so that the committee had the advantage of hearing multiple perspectives. It won't be a complete set, but we structured it so that we have various points represented, and we complicated matters by putting in some real life examples into the panel.

So the way to get a lot of information out at the same time is we asked them to provide written testimony. That's in your packet. And, for the public, that was posted on the Web site before today's meeting. And then we'll have five minutes, sort of high points from each panelist, and then have plenty of time for the dialog between the committee and the panelists. So with that combination of opportunities, we're hoping to get a lot of information on the table. As David mentioned, this is an informational hearing, so this is the first state of trying to get information out. Paul.

Paul Egerman - eScription - CEO

Yes, thanks a lot. And also, if you're watching on the Internet, and you want to know why you're not seeing any PowerPoint slides, it's because there aren't any. So there'll be just five minutes of presentation followed by questions and answers. We have four individuals sitting at a table here who are extremely prominent in their areas, and in addition to giving very short opening statements, I'm also going to give each a very short introduction that will not do justice to their backgrounds.

Our very first speaker is Deborah Peel. Dr. Peel is a practicing physician and a national expert on medical privacy. She's the founder and chair of Patient Privacy Rights, and also founder of the Bipartisan Coalition for Patient Privacy. Dr. Peel.

Deborah Peel - Patient Privacy Rights - Founder & Chair

Thank you for that introduction, Paul. Thank you to the committee for giving us this opportunity to testify today on behalf of the millions of Americans who are very concerned about the problems of who controls data in electronic systems. In fact, control over personal data is the major concern American's have about electronic health systems.

We appreciate all your service. We appreciate that you're having this hearing today. I do have to say that we really think that the cart is in front of the horse. Plans have already been made and been worked on for many years, standards, as well as the plans developed by this committee. And we think that actually the privacy issues are foundational and really belong at the beginning because insuring control over data is really the only way that we're going to get to a trusted health IT system. In other words, building the kind of system that Americans have been used to for over 200 years, which is a system where they trust their doctors not to share data without their permission.

Any discussion of privacy has to start with three crucial facts, and the first one is that Americans care very, very deeply about privacy and control of their information. And what we did today was draw on the new report from AHRQ. It just came out. They studied people's attitudes about health IT and research and fears about data, fears about electronic systems across the nation. They had 20 focus groups, and I'd like to summarize them. This is in our notes.

There are four major points. The majority of Americans think that they should own their health data. The second point, there is universal agreement that they should have, Americans should have a say in how this information is shared and how it's used. The third point, a majority believe that no one – it's no one's

business to know about their personal health information, not because they're concerned about a specific kind of disclosure, but as a broad principal. It's personal information. It's mine. I should have a right to keep it private. The last point that they found was that the participants overwhelmingly want to communicate with their providers about how their data is handled and shared and for what uses, what purposes. And they automatically believe they should have the right to correct misinformation.

A further point that we want to make that I think many of you know about is the famous California healthcare survey of 2005 that found that 13% to 17% of Americans are already taking action to hide or omit data from the healthcare system. And again, this was in 2005. I don't think the same questions have been asked since then, but if they were to be asked, I wonder if the results would be even higher because people's concerns are growing. They're not receding.

Then, finally, we wanted to bring your attention to the studies that were done on behalf of the Institute of Medicine by Allen Weston, and his survey found that there's really only one percent of Americans who would ever agree for researchers to have unfettered access to their health information, one percent. Further, he found that four-fifths of the population oppose having their information used without their permission, even if it's de-identified and even if it has IRB approval. And yet, 87% of Americans support research. The point really is, they want to know and they want to be asked.

Our second major point is that the right to privacy, the right to control personal health information is the national consensus. This has been developed in all 50 states over 200 years. This follows from Hippocrates and centuries of medical ethics. But the idea that we don't have a consensus in this nation about who should control health information and the right to privacy is not correct, and one of the things that we submitted to you as part of this report is a document by Jim Pyles, who is a lawyer that has worked on behalf of consumers' privacy rights for many years now, laying out the constitutional rights, the rights in common law and state law and so forth that are very, very high standards, again part of the national consensus.

And in the HRQ report, another key finding was that the public does not support having general rules, one rule, one size fits all in terms of privacy policy, and that everyone should have the right to determine their own standard. The good news is technologies exist now to allow that. Again, in our fuller materials, not only today, but our coalition has written two or three other letters to this committee, and a letter to the standards committee, laying out in detail examples of privacy enhancing technologies and systems that exist now that are in use now that have been successful.

Our third point is that privacy, meaning again consumer control over data is the cheapest, easiest, and most efficient way to insure that data flows. The person with the clearest right and ability to say I want my data to go from this place to that, from this hospital to that researcher, from my PHR to that new physician is the patient, is the individual. So we need to keep this in mind as we move forward and think about the NHIN system, distributed systems, and complex ways of sharing information. The cheapest way for it to go without the need for expensive, complex legal agreements is asking the patients.

Fourthly, consumer control is the one way to insure that all the stakeholders cooperate. There's tremendous stakeholder resistance to sharing data. Stakeholders believe they own our data. But the truth is, the only person again who can make the data liquid, who can end the data blocks, the data silos is the patients. Why not ask the patients. Again, I think, as Allen Weston's research showed, the public wants to provide data for causes and research they believe in. They want to know about it and be informed about it.

Today we're asking you to set a really high bar for privacy. We're asking you to meet Americans' expectations of what it will take to trust these systems. We're asking you to set this bar because there's no question that the data mining secondary and tertiary and so on, uses of health information is a multibillion dollar a year business. The data mining industries are not going to change. They're not going to reform unless you give them clear direction.

This isn't the case just with health IT, but if you think about progress in many areas of our economy, change only came in industries when it was mandated. The auto industry didn't improve fuel efficiency until Congress mandated it. It took mandates to get the lead out of paint. Industry doesn't want to change, and the major industries today don't want to change and build the system that's trusted.

I guess I want to talk a little bit about the fact that healthcare is not a system. It's really a two-person enterprise, and if one person is unwilling to walk in the room and share information, we won't have data. Data can't be compelled, and so to kind of wrap up, we're asking you to remember that people need to be able to make informed consent. They need to know what's going out to whom and for what purposes, how long. They need to know in a meaningful way what they're consenting to and what's been disclosed. They need to correct the information so it's not erroneous, and again, the good news is systems that provide this are already here.

As far as policy, we're asking you for three simple ideas, three simple policies that would make the system work, overriding policies. One, no protected health information should be exchanged without informed consent. Two, the patient should have a right to designate a place where their provider can send an electronic copy of their data at no charge. Three, all access to patient records should be with explicit permission, informed consent, and that means that patients have to be able to selectively segment sensitive information, and it means we need segmentation and audit trails now so that we can prove that data is handled in the way that patients want. Thank you so much, Paul.

Paul Egerman - eScription - CEO

Yes. Thank you very much, Dr. Peel. Our next speaker was supposed to be John Rother from the AARP. Unfortunately, at the very last minute, he was called away and was unable to come, but we managed to get a pinch hitter, which is a member of the policy committee, Deven McGraw. We, around 9:00 last night, roped her into this job, and Deven, as you know, when she's not very busy helping us with the policy committee, is also with the Center for Democracy and Technology.

Deven McGraw - Center for Democracy & Technology - Director

Thanks, Paul. It's not easy to do this at 9:00 at night. This was a bad week to adopt a puppy. Let me tell you a little bit about CDT, so you know where I'm coming from, if you don't know. The Center for Democracy and Technology, where I work, is a nonprofit, public interest organization that's here in D.C. that was founded about 15 years ago to promote democratic values and individual liberties in the digital age, and the organization has a long history of expertise on Internet and information privacy issues.

The health privacy project, which used to be an independent organization, has more than a decade of experience in advocating on healthcare privacy issues. And, about a year and a half ago, we merged the two in order to sort of leverage the expertise of both to deal with the movement of electronic health data onto the Internet and electronically. And so really what we try to do is to think about and recommend really workable solutions to better protect the privacy and security of health information online.

Consumers absolutely want privacy. I wouldn't reiterate at all what Deborah said. She covered it really well. But they also want their data to be accessible and used to treat them, and they want to be able to get access to that data themselves. So there are many issues to consider, as we figure out what are those workable privacy and security solutions.

Again, I won't go into detail on why we need to focus on this. I think, obviously, we all appreciate that or we wouldn't be here today. But what I do want to respond to is the particular solution that she advocates, which is protecting privacy by giving patients more control of their data, which means requiring consent for each and every use. And it's a really intuitive and appealing solution, and it absolutely doesn't surprise me that people in focus groups and in surveys say give me control of the data. I don't know that anyone, other than maybe some folks within the healthcare industry or healthcare experts, would answer those questions any differently. Being in control of something feels intuitively better.

The problem is – and, of course, giving patients some control over their data is in fact an important element of privacy protection. So while basically what I'm going to tell you is consent doesn't work as

well to protect privacy, as we would want it to, and we need to do something. We need to focus, in particular, on creating a comprehensive framework of rules, and then also putting consent in, in certain instances, where there is value for doing so. You know, never the less, what I'm mainly going to focus on today is why consent in fact doesn't work. We wished that it did, but in fact over reliance on consent provides very weak privacy protection.

We've written a paper on this, which is on our Web site, which I'll make sure is available to the committee as my testimony, but I'll just sort of try to summarize that here. It's not easy. It's about a 20-page paper.

Really, the limits of consent were actually illustrated pretty well in something that hit the news not too long ago, which was there were reports about health and life insurers obtaining personally identifying prescription drug information from commercial data miners and using it for a range of purposes. This revelation, of course, was cause for much consternation, but in fact that data was in the hands of those entities because, in each and every instance, the patient consented for the data to go there because they didn't really have much of a choice. They were applying for insurance, and when you apply for something, you have to consent to the use of your data for those purposes. Healthcare doesn't present us with good opportunities in a lot of cases to provide people with a meaningful right to say no, and that's one of the reasons why consent, even though it's incredibly appealing and intuitive, doesn't tend to work very well to protect privacy.

Equating privacy with consumer consent relieves the holders of patient data of the responsibility for adopting comprehensive privacy protection because it puts the burden for protecting privacy on the consumer and takes it off of the entity. If the industry were directed simply to solve privacy concerns with consent, there'd be far less incentive to design and implement systems with technological and operational protections for privacy. In other words, if I can rely on a consent form to authorize all potential uses and disclosures, why would I bother to design a network in a way that minimizes risk to privacy or spend really scarce resources on insuring that systems incorporate the latest security technologies, or train staff on what are the permitted uses and disclosures of information.

Let's get the patient to tell us and authorize the use of their data when they need healthcare or when they're signing up for an insurance plan. It's easy to see how, notwithstanding that the concept of control is very appealing, it just doesn't work in the way that we would want it to. We don't want the role of enforcement of privacy to be relegated to a mere, well, did the form that the patient signed, no matter how detailed, no matter how simply stated, authorize the use of this particular information? And if it did, that's the end of the inquiry.

I actually was at the HIPAA summit yesterday, and compliance lawyer actually was telling folks the best way to be certain that you're using information appropriately is just get the patient to consent to it. It surprises me sometimes that this notion of consent for everything doesn't actually, isn't actually appealing to industry because, in some respects, one might consider it easier than figuring out how to comply with a complicated set of rules. You know, privacy policies are not written typically in language that people understand. A lot of people don't read them. They use general. Even if they're simply stated, they use general language. From time-to-time, we will use your data in ways that will improve your healthcare and lower your costs. Who's not going to sign up for that? But it doesn't tell you very much about how data is used.

Similarly, if there are categories of information that you're asked to consent to, research, healthcare improvement, healthcare quality improvement, even trying to segment it down at the category level, there's sort of a wealth of information that's subsumed in there that the consumer is never going to fully understand. Again, if it worked well, we'd be the first person, one of the first groups up there advocating for it, no matter how complicated or costly it would be. It's not about whether it's too burdensome. It's about whether it works. And, unfortunately, it doesn't.

Just because consent, you know, over reliance on consent doesn't work, again, doesn't mean that there isn't a role for patient consent. We actually think that there is. It needs to sort of be layered on top of this comprehensive framework of rules that govern how entities use and disclose information, and two areas

where we could stand to strengthen consent would be one with respect to health information exchanges, particularly where that business model is in flux, and particularly where the uses and exchange of data is for more than treatment purposes. And I know that Gayle mentioned opt in, opt out. I suspect that will be an issue that will be worth pursuing. I happen to think that that's the case.

Personal health records where you're talking about a record that is a copy of an electronic medical record, and for the patient to use. There's a strong case to be made that individual consent over that record, that that record belongs to that individual, and our public policies really ought to reflect that, and they don't actually at this point, at least not in a universal way. I think that I will provide one more example on the consent thing and then stop so that others can have a chance to testify, and then we can take questions.

Our e-commerce marketplace provides a really clear example of why a comprehensive policy framework to govern data use works so much better than consent alone to establish trust and make sure that information can be shared. Today, most of us, there are few who do not, but most of us use credit cards and show online or bank online. And these systems work because we have rules in place that govern who can access that data, that require for there to be security in place, and that hold the individual harmless or provide some sort of compensation for them if in fact there are errors. It doesn't work and there isn't trust because patients consent to each and every movement of the money, as it goes through the system. With that, I'll close, and thank you for the opportunity. I apologize if this went over. It was a little disjointed, but I'm happy to answer your questions.

Paul Eggerman - eScription - CEO

Thank you very much, Deven. The next speaker is Marc Overhage. Dr. Overhage is the director of medical informatics at Regenstrief Institute. He's also a professor of medicine at Indiana University School of Medicine, and he is the president and CEO the Indiana Health Information Exchange, IHIE. Dr. Overhage.

Marc Overhage - Regenstrief - Director

Thank you and good morning. I'm pleased to be able to provide the committee with a brief case study of how our health information exchange, over the last 15 years, has approached patient engagement in general and individual choice in data ... specifically.

The Indiana Network for Patient Care or INPC, which has been operated and developed by the Regenstrief Institute starting in 1994, provides health information exchange across the state of Indiana. And along with our docs for docs clinical messaging platform operated by the Indiana Health Information Exchange, supports health information exchange for over 10 million patients, 12,000 physicians and their staff. Approximately 50 hospitals participate in the INPC, along with independent laboratories, radiology centers, payers, pharmacies, public health and others.

Patient privacy and the security of their health information are and have been fundamental to our health information exchange since its very beginning. We've architected the privacy and security into the software, the processes and the agreements from the ground up, with a careful attention to the balance between them. Our health information exchange and its partners, the clinicians and providers, subscribe to and implement the principals described in the Marco Foundation's connecting for health framework, specifically openness and transparency, purpose specification and minimization, collection limitation, use limitation, individual participation and control, data integrity and quality, security safeguards and controls, accountability and oversight, and remedies, motherhood and apple pie.

How do we try to attack that? First of all, by adhering to these principals really requires not just the health information exchange, but the providers to work in concert. The participating providers must have executed the INPC participants agreement, which requires them to follow certain specified security and privacy safeguards within their organization. These legal, process, and policy structures are critical to insuring that the privacy and security of patient's health information. Providers inform patients initially through their notice of HIPAA privacy practices how the provider intends to use the patient's data. This

notification is a primary opportunity for the patients to become informed by discussing with their providers their wishes around the use of the sharing of data.

Our technologic underpinnings have been designed to support these principals as well. The technological infrastructure underline the INPC as a centrally managed federated database model. The provider stores data for which they are the custodians in a database that they maintain in a standardized structure in standardized format. The patient's demographic data from the encounter is used to create what we call a GPI or global patient index, and that's global only in the sense of the participants, not the world, that links patient identification together across the different participating providers. The system uses that GPI to create a virtual patient record from the participating provider's databases when appropriate conditions are met to enable access for a specific use case. These requirements or limitations are decided upon and designed by the INPC management committee. These highly specific conditions insure appropriate limitations on use.

I'll give you one concrete example. In order to create a virtual patient for a record when a patient presents to an emergency department for acute care, first of all, the participant in that emergency department, the organization must have agreed, through their contracts with the other participants, that they will follow the specified security and privacy safeguards internally. The INPC system has to receive the secure notification that the patient has presented for care at that specific facility. The physical device, the computer if you will, from which the clinician is trying to access the patient's record must verifiably be present at that facility's location, that specific facility, not just within the healthcare system.

The provider trying to access the system must authenticate themselves to the systems, and must have previously been authorized by that institution or healthcare system to access data for that specific use case, emergency care in this example. Finally, the access time or limitation on how long that virtual record can be created for is limited to 24 hours after the patient presents for care on the presumption that very few episodes of emergency department care will extend beyond that time period. So different conditions would apply for different use cases. For example, creating a virtual patient record for a primary care provider in the ambulatory setting or for public health reporting.

Any time a virtual patient record is created, an audit trail is created and maintained permanently of a variety of data related to the access, which information from which institutions, which user accessed the data, and so on. And that information is available to the patient through their provider.

Providers who participate in the INPC decide with their patients which data are made available in the provider's health information exchange database. The INPC founders have designed the INPC to recognize the importance of the provider/patient relationship, and we believe that the patients understanding and control of his own data should be a topic of discussion between the patient and the provider in which the patient has placed his trust to provide their care.

Philosophically, we don't believe that these decisions and discussions should occur with the health information exchange, but rather with the provider. If a patient and their provider agreed that it is in the patient's best interest for certain data not to be shared, the provider is required by their INPC participation agreement not to make that data available in the health information exchange database. The provider who maintains the direct relationship with the patient then notifies the INPC of the patient's request, and the INPC staff flags the patient in the GPI so that the system can enforce the patient's desire should they choose to completely opt out or decide not to participate.

Similarly, patients who identify corrections or clarifications that may be needed in their health information work with their providers so that those corrections are made in the source systems and are then promulgated to the exchange. Insuring the security and privacy of patients health information requires careful attention to all of these principals by both the providers and the health information exchange, and within a comprehensive privacy protection and architecture – excuse me – privacy protective architecture in a networked environment. Thank you for the opportunity and look forward to the discussion.

Paul Egerman - eScripton - CEO

Thank you very much. The final speaker is Susannah Fox, who is with the Pew Internet & American Life Project. She is a frequent contributor to a blog called e-patients.net. The most recent article is called HIPAA's broken promise. Ms. Fox.

Susannah Fox - Pew Internet & American Life Project - Associate Director

Thank you. The Pew Internet & American Life Project is funded by the Pew Charitable Trust, which, as you know, is 19th century Pennsylvania oil money. We have no connection to technology, and I think that's important to note because so much of what we do is in studying the social impacts of the Internet goes toward ideas that are central to policymaking, and yet we don't advocate for any policy outcomes or have any positions on policy. What we do is try to provide an accurate picture of a changing population.

And now that we're going into our tenth year of surveys about how people use the Internet, I can say that we have learned sometimes the hard way that it's important to focus on people's actual behavior, not hypotheticals, not attitudes, because as we've seen even just in the last couple of years that people will say one thing and do another. So what I am hoping to bring today is some insight based on what we see people actually doing.

I've focused on how people use the Internet to gather health information. What we saw in the early days of the Internet is that patients would route around doctors who, back then in the '90s, would warn patients away from using the Internet. Patients wouldn't listen to that. They were gaining so much from what they found online that they would essentially change doctors or go underground. They would work outside the system. We're seeing some of that, again, where people are unable to get what they want from the current healthcare system, essentially for all the reasons that we know, and so people are going outside the system, creating their own ways of gathering and sharing health information.

And what I'd like to urge you to do is learn from the data that we have and other researchers have to create a system that brings those patients in. Why not create something that allows patients to collaborate with doctors and contribute to healthcare? And privacy and security are absolutely foundational requirements, but not the end goal. Health is the end goal.

What I wanted to talk about is how what we're seeing in our latest data is that the American people have a different expectation about access to information. We've seen a change even just in the last two years. There's a new ... where people feel that they should have access to what I think of as industrial strength information, not consumer strength. People are, for example in the political campaign, we're watching the actual speeches. They were reading the campaign papers that were available online, not just reading what was in the newspaper or watching TV. In terms of healthcare, people are accessing medical journal articles, not just waiting for the summary that's available in mainstream media.

What I would say also is that I'm here today representing sort of a consumer voice through my survey data, but also I wanted to read some comments that I got on the e-patients blog last night. I posted my testimony and said what else would people like me to say, and so you have my prepared statement. You can check that out. All of my research is available on the Pew Internet Web site, but here's what people had to say when I posted it.

e-patient Dave Debronkart wrote, I want innovation at a rate that resembles the rate of improvement in cell phones and iPods. I want to think in 2011 that the healthcare tool I started using in 2009 is, well, that's so 2009. Just the way many people think about their cell phones. And he echoes what Dr. Peel said. You bet I ought to be able to get my hands on all the data and proofread every last bit of it, show it to my own selected experts, and take it with me wherever I want.

Another comment that I go was actually quoting from HHS report expanding the region impact of consumer e-health tools. And the quote is, consumers with diverse perspectives, circumstances, capacities, and experiences must be included in the design of and have meaningful access to evidence based culturally sensitive e-health tools. That's in response to the part of my prepared statement that talks about how mobile Internet access is erasing the differences that we see between white adults and African American adults in terms of our definition of the Internet user population. Please include mobile in

whatever you decide to do because that really is the future. Eighty-five percent of American adults have a cell phone.

The third and final comment that came through on the blog last night, I think is a really interesting one, and goes to some of what I've seen in your previous discussions, and that is that patient generated data represents a new pool of research data that has the potential to improve comparative effectiveness studies. ONC, HHS could help establish standards for data quality for patient generated and outcomes data. I think that's where we're going, so when we talk about where we are now, we're talking about the Web. Where we're going to be, we should talk about mobile. Where we're going to be, we should talk about patient generated data. That's where people are working outside the system at this point. We should welcome them in and harness the power of so many people who want to contribute to healthcare. Thank you.

Paul Egerman - eScription - CEO

Thank you very much. These are some fascinating comments, and also a diversity of comments on a number of issues, including the role of consent. And I think now we're going to open the discussion up for questions and comments from the committee. Paul, are you handling this part, or am I doing this part?

Paul Tang - Palo Alto Medical Foundation - VP & CMIO

Go ahead. Yes.

Paul Egerman - eScription - CEO

And so, yes, I will be facilitating that, so people should raise their hands if they would like to say something.

David Blumenthal - Department of HHS - National Coordinator for Health IT

...has figured out a new way to lighten his burden.

Paul Egerman - eScription - CEO

Absolutely. But since I'm doing that, actually the first person I would ask is Christine, if you had any comments about what you've seen because I know you've done a lot in this area.

Christine Bechtel - National Partnership for Women & Families - VP

Sure. Thanks, Paul. First, thank you to all of you for the fabulous though work that you've put into this panel, and I'm grateful for the design of the panel that it includes such a comprehensive range of reviews. I actually have a couple of things.

I wanted to start by asking Marc about the accounting of disclosures and how, if you could talk a little bit more about that. I know that there are a range of views out there, particularly given the changes in ARRA, and I think we're going to hear later from people who have some concerns about the volume of data and the granularity. So I think I want to ask two things. One is, how are you handling those changes, and what is your perspective on the appropriateness of those changes per ARRA? And then the second piece of that is, how you're facilitating those conversations at the patient provider level so that patients can understand more about what they can understand about how their data is used and disclosed.

Marc Overhage - Regenstrief - Director

Thank you very much for the question, and I think it's fair to say that our general approach is that this is an issue between the patient and their provider because they're the custodians of the data. And so as you pointed out, we facilitate in our various venues, our management committee discussions, and in other venues this broad topic of disclosure with providers, which they have to deal with independent of any issues around sharing or health information exchange in any form.

We facilitate that disclosure, but aren't involved in it as the health information exchange because, frankly, we have no relationship with the patient, nor can we appropriately authenticate the patient. If somebody knocks on the health information exchange's door, how do we know who it is? We believe that belongs

with the provider and the patient. And then we facilitate with the provider access to that information as the provider and the patient decide by providing the audit logs and disclosure information to the provider who can make it available to the patient.

Christine Bechtel - National Partnership for Women & Families - VP

Okay. So can I ask one other for Deven and Dr. Peel? Both of your presentations were compelling and very helpful. And I think one of the things that is striking to me about the role of consent is that when you talk to patients and their family members, oftentimes what you hear, and we heard this in recent focus groups that we conducted, is that they overwhelmingly want to share information in the context of treatment and in the context of care coordinator in particular. The '05 California Healthcare Foundation survey that you referenced, Dr. Peel, reinforces that. I think it was 98% said that they wanted that.

But I think it becomes a different conversation when you talk about privacy in the abstract. And, of course, as Deven pointed out, everybody wants control. So as we think about the need to walk the right line and really actually probably more of a circle that will encompass the right level of controls for people, but at the same time, given them what they want, which is high quality, patient centered healthcare. I'm wondering about whether the role of consent should really focus particularly on those areas like healthcare operations where it's a little bit more squishy, the definition, and broad versus changing the framework that we do have in place today, which is built around HIPAA for particularly treatment, I'm thinking. So I want to ask you guys your perspective on what we need to focus on in healthcare operations in particular and how that can be part of the comprehensive policy framework that I really hope this committee will begin today to tackle.

Deven McGraw - Center for Democracy & Technology - Director

Healthcare operations, for those of you who haven't seen the definition, is essentially a bit of a list of sort of what I sometimes refer to as back office activities that healthcare institutions often need data for. And from a consumer advocate's perspective, it's perplexing because some of them are really broadly worded. In order really to give hospitals and doctors and health plans a fair amount of discretion to be able to use the data to do their business operations. I mean, healthcare is also a business. So, to some degree, there is a need to be able to use some patient data in order to function on a daily basis.

On the other hand, we don't like big broad categories that say things like administrative activities and other things related to healthcare. I don't have the definition in front of me, but some of the prongs are more specific than others, and it's always been a really troublesome category. On the other hand, if consent is not a really good privacy protector, it wouldn't work all that well in operations either. And so my own view is that I'd much rather provide incentives for entities to be good data stewards when they use data for operations such as not always using it in fully identifiable forms, so just to pick one out of a hat. Credentialing of doctors requires the use of data about how well they've provided treatment. But you don't need to know that that treatment was of me. You just need to know the certain pieces of data that can allow for their peers to judge whether or not they were providing appropriate care.

I think it's tough because you look at that laundry list, and you say, oh, come on. All of this stuff without asking me? Again, it is intuitive, that control piece of it, but if you ask patients to consent, and again in an environment when they don't really have an ability to say no, you're not going to get any better privacy protection of that data in my view.

Paul Eggerman - eScription - CEO

Did you want to say something, Deborah?

Deborah Peel - Patient Privacy Rights - Founder & Chair

Yes, I do. Thank you. Well, certainly we agree with Deven that healthcare operations are a very troubling category. In fact, that's the main category of open use by providers for data for any purpose that they would want, including the sale of data. And so we certainly believe that, again, if the healthcare entity like a hospital can explain in a clear, simple way how they want to use the data, and it makes sense to people, people will agree. People will agree to business uses if they make sense, so that's certainly the most troubling category.

But there are several points that I really do need to rebut that Deven said. I mean, the idea that consent doesn't work, you know, I have no idea where that's coming from. There is no such study. There's never been any, and any kind of research that I know that shows that consent doesn't work. And when you're talking about consent not working, you are essentially always talking about coerced consent or blanket consent or situations where people have no choices.

You were talking about the trust in the e-commerce situation. Yes, we trust that banks, etc. handle our money the way we want them to. But we have no privacy over our financial records. I'm sure everyone is aware of that. We don't have the right to consent to the fact that they sell and use our financial records. I mean, the problem is that we don't have meaningful consent over all kinds of uses of protected health information that have nothing to do with healthcare, nothing to do with healthcare, have everything to do with business models and profits from health data mining industry.

And so, if we're going to talk about consent, and I tried to say this briefly, consents have to be meaningful. They have to be informed. That's the legal standard in this nation. Informed consent, you have to know what you're consenting to and what it's for. Now whether consents would turn out to be burdensome or not, and Jodi is talking about studies finally being done about that. That would be great, but we pointed to in our testimony today and in other written testimony we've submitted. The fact that very detailed consents have been working extremely effectively for the exchange of sensitive data.

I'm a psychiatrist. Some of you know this. You know, everything is about privacy in the mental health field in particular because no one would tell us anything if they thought it was going to be broadcast. For those of you who haven't heard me say this before, I learned about this issue from my patients, literally when I hung out my shingle, people came in and said, if I pay you cash, will you not disclose my information because they'd already been hurt, and we're talking about jobs here. This is about jobs. It's not about marketing. It's about opportunities in jobs.

And so we know that the NDIIC is a national open source consortium that's developed very effective, granular consent for the exchange of sensitive mental health data. They've been doing this for eight years. They've exchanged the data on four million patients. It works fine. The data goes where it needs to go to help patients, and it has not been an obstacle whatsoever.

By the way, those are standards for consent that exist that are very easily translated with HL-7. The fact that the standards committee is saying we don't have consent standards because they've got blinders on. They don't want to see what's out there and what's working. We do have standards. We do have things that could easily be used throughout the system.

And here's the thing. In order to insure segmentation, in order to insure that we're going to be able to do genetic research, we're going to have to have a system of consent that's trustworthy that allows sensitive information of all kinds to be segmented, and so we're going to need consent. We're going to need audit trails. We're going to need them now.

Again, to clarify, patient privacy rights in our coalition doesn't believe that we shouldn't have data security, that we shouldn't have a framework for trusted exchange of data, and that we shouldn't have framework for confidentiality and trusted stewards. But the stewards should do what the patient says with the data. That's what stewardship is about, not what's good for the institution, but for the patient. And so, you know, again, we are – you can't have – it's meaningless to say you have control of your data if the system is not secure because anybody can get into it. So you have to have security. You have to have meaningful framework, but you have to have patient control.

Paul Egerman - eScripton - CEO

Great. Thank you. We have questions from Frank and then Gayle, so first Frank.

Frank Nemic - Gastroenterology Associates - Gastroenterologist

Thank you. I appreciate.

Paul Egerman - eScription - CEO

Can you say your whole name for us?

Frank Nemic - Gastroenterology Associates - Gastroenterologist

Yes. Frank Nemic, a gastroenterologist. You know, in our practice, we've been very conscientious about patient confidentiality, that if someone is not on a HIPAA form, that information won't be disseminated. In the two years since we've had an electronic medical record in our practice, it's really been easier to implement the HIPAA protocols because it's more readily available.

But the problem with confidentiality was really eroded many years ago with third party payers. The patients understand that everything they tell me can be transmitted to the insurance company, and they also understand that all of my recommendations to them will also go to that insurance company. There was no consent. As a condition of being insured, they have to agree that that information will be transmitted to that company, to that company of people they don't know. They don't know who the claims reviewer is or how that information is processed. They have no control over it.

Patients have lost their privacy many years ago. How do we get the genie back in the bottle?

Deborah Peel - Patient Privacy Rights - Founder & Chair

I'd love to answer that. Patients gave consent for the information to be used for one purpose by the insurers and one purpose only, to make a determination about how much they're going to pay the claim. The problem is the insurers turn around and use that data in many other ways that patients are never informed about, never told about, and that's quite harmful to them. For example, sharing that information with employers or aggregating and selling that data to major employers in forms that can be re-identified.

So again, this really gets to, if you will, the code of fair information practices that was developed years ago by the predecessor to HHS, the Department of Health Education and Welfare. And one principal is that we don't have control, but it's because our control has been stolen. When you give consent for your data to be used for one purpose, that should be it. It should stop there, and then if the insurer wants to do something else with the data, they should have to come back and ask you. This is the principal of single use. That's why we have no privacy. That's why we have a giant secret data mining industry, health data mining industry in this nation because the information is so useful.

And today, in fact, I brought something to pass out to you. Today, HIPAA allows all of these entities that touch your data to go ahead and use it for other kinds of purposes. Many people don't realize that HIPAA was gutted in 2002, and the control over data use passed from the patient and the individual to all of the holders of data to make the decisions when they want to use our information. You know, I think this would be relevant to pass around.

Paul Egerman - eScription - CEO

Okay. Thank you.

Deborah Peel - Patient Privacy Rights - Founder & Chair

What had happened is a single sentence that changed the HIPAA privacy rule into a disclosure rule.

Paul Egerman - eScription - CEO

Thank you, Deborah. Are you all set, Frank?

Frank Nemic - Gastroenterology Associates - Gastroenterologist

Yes, sir. Thank you.

Paul Egerman - eScription - CEO

Great. Gayle?

Gayle Harrell - Florida - Former State Legislator

Thank you very much. First of all, I want to thank Dr. Blumenthal for having this open hearing today. I think this is the most significant and most important thing we are doing as a committee. Not only are we opening the whole conversation we've had many on meaningful use and many on certification and HIE, but this is absolutely the foundational question, not just for how we're going to move forward with electronic health records dealing with privacy, but we've opened the door.

The genie is out of the bottle, and it has been out of the bottle. I think we really – this is opening a conversation that really is a very – needs to be a very public conversation on how we really are going to deal with the privacy and security of these records. I have a great deal of concern on the business association aspects of privacy and security. Deven, I couldn't agree with you more when it comes to consent. Coerced consent is the worst thing for privacy and security that I have seen, and I would like the panel to really look at the business association relationships with when that data travels from the physician's office or from the hospital. And then is used again and again by other business associates. And you can go down three or four chains before you come to that information being used out there, being sold and being used.

And individuals have a great deal of concern. This is the number one concern I hear with electronic health records. How is my information going to be used? They're also afraid that things are going – that the systems are going to be broken into, and that comes to the security aspect, which I'm sure we'll get into as well. But I'd like to hear some comments from the panel on business associates and the use or misuse of information.

And I'm looking for solutions. I'm a solution-oriented person. Give us; give the committee direction. If you were queen for the day or king for the day, what would you do to protect this information?

Deven McGraw - Center for Democracy & Technology - Director

Thanks, Gayle. You know, we did actually. We do have some provisions, as Jodi showed us in the beginning, that sort of strengthen enforcement of the HIPAA rules on business associates. But having said that, I think we do have another problem about the way that data travels down the chain. I fully acknowledge it, and I agree with Dr. Peel that this is something that we really need to get a handle on, and it's not addressed by what happened in the economic recovery legislation. Essentially some of this is anecdotal reports that we're getting, but business associates getting data from one covered entity, and then it's as though that data belongs to them, and using it for a range of other purposes.

The way to fix that, we think, is through stronger rules on what business associates can do with data. That if they're receiving data from a covered entity, that data isn't theirs to then use as they choose to meet their own business objectives. But instead, they perform the function that they've been asked to by the covered entity, and that's the end of the story. They have the data by virtue of that relationship. They cannot then turn around and assume that they can use it for any other purposes. And so I think the law is there, but it's just not clear enough, and it hasn't been appropriately enforced, and we could do a lot to clarify that and improve our enforcement there.

Paul Egerman - eScription - CEO

(Inaudible.)

Frank Nemic - Gastroenterology Associates - Gastroenterologist

Thank you all very much. First, just, Susannah, I want to just reiterate the appreciation the comments for patients having control and actually being the ones submitting a lot of this data. I think patient reported outcomes are going to be critical, particularly in my world of cancer, but also having the power to take what's in their electronic records, either their doctor or them, whoever, saying I want this data out there.

But I have a question more for Deborah. Deven, I'd like your comments as well. It does deal with somewhat the consent issues. Cancer is so linked to research, and it's ongoing. We're learning this is hundreds of diseases. It's not necessarily body parts. You mentioned genetics. It really is a molecular disease. So there's clinical research data. There's public health research data, constant monitoring.

We're now identifying. We are thinking more and more all cancers are subpopulations. There are going to be responders. There's not going to be responders.

The Moffit Cancer Center has put together this total cancer care program where they are getting their patients. They're profiling them. They're doing molecular profiles. They're getting the bio specimens, all the cancer bio specimens. They're putting all this in databases, collecting data to see what works and what doesn't, building a learning comparative effective research profile so that doctors can go in and look years down the road and say, you fit this profile. This works well for you.

Subsequently, it's going to align them with clinical trials. We're going to find out what molecular markers may make you a responder, not a responder. All of this is going to require constant, going back and forth between the patient's data, monitoring, going to the bio specimens, and conducting research. So after that longwinded response, what I'm wondering is do we only need one consent at the beginning to participate in large-scale programs? I see you're shaking your head a little bit. I guess my concern is, at what point does it become so cumbersome that we really can't conduct research on this.

Deborah Peel - Patient Privacy Rights - Founder & Chair

Well, certainly that's the big fear that somehow consent will interfere with research, but what people forget is how easy and cheap technology makes it to contact people. It might have made sense decades ago, if you went into the Mayo system, to give consent for the use of your data forever, you know, in perpetuity because it could be very difficult to contact you, time consuming, expensive, etc. But people forget that technology could enable you to be pinged on your cell phone. I mean, technology eliminates most of the burden of getting in touch with people easily.

So the cost to connect, the cost to give consent are very different now in this new environment. In fact, part of the reason for IRBs were set up because it was difficult to contact large numbers of patients and get their permission for things. Guess what. It's not difficult anymore when 85% of the adults have cell phones, when this government has proclaimed every one of us will have an electronic health record. It's going to be very easy to get ongoing, contemporaneous, informed, meaningful consent.

Now does everyone want that? No. Everyone doesn't want that. The people that want to give blanket consent for future research because, let's say, I trust Moffit. I love Moffit. I think they're going to do great security. They're going to have great doctors. I'll be a little bit of a shrink. Positive transference to Moffit. I think they're wonderful. I want to give it to them. You can still do that. You can still do that with consent management systems. You can give broad directives, but before you give a broad directive like that, you should be informed about what the potential consequences are, not just for your life, but for your children, your grandchildren, and your relatives, that kind of thing.

And so people are going to have different preferences about how often they want to be contacted or for what purposes. And the ones that want to give broader directives to their own physicians or to their own hospital in Austin, Seaton Hospital, you know, they can do that. And then those that don't want to, don't have to. And that was the findings of AHRQ is there isn't one size fits all, and that's what's so fabulous about innovative technology. We no longer need black and white, opt in or opt out. We can do very selective segmentation, which is on the table finally. And with audit trails, we can be sure that whatever we say doesn't go, does go, and what does go does go.

But that's the beauty of technology, and they exist today, and we hope that you will – in fact, we've submitted a list of names of panelists that can talk about these things that are working now. And there are some great one, consent mechanisms to allow selective information to go to researchers as well. There's some great stuff out there.

W

...the source of the 85% have a cell phone. A lot of people don't turn it on every day, and a lot of people still don't know how to do text messaging, so I just want to clarify that while we do have a very high penetration, there's definitely gradation in actions that people take.

Paul Egerman - eScription - CEO

Terrific. Michael?

Mike Klag - Johns Hopkins Bloomberg School of Public Health

Mike Klag. So Dr. Overhage, I have a question for you. The system you described, the network you described has many of the characteristics that some of the panelists had suggested as good characteristics of the system. So can you tell us of the – you have 12,000 physicians and 10 million patients. Of those 10 million patients, what proportion is that of all the patients that are seen by those physicians, so how many give permission to be in the system?

Marc Overhage - Regenstrief - Director

Thank you. We aspire to do the best we can, and the practical things are often challenging, and we just keep trying to do the best we can. The ten million patients, there are only six million people who live in Indiana. Some of those patients are dead. Some of those patients are patients – well, no, they are. Some of those patients are—

Mike Klag - Johns Hopkins Bloomberg School of Public Health

Are you...?

Marc Overhage - Regenstrief - Director

...well, that's a whole other topic in a different office. Some of them are folks who have transited through the community and seen at the Indianapolis Motor Speedway Hospital, for example, during the Indianapolis 500. No, those are very real things.

Of those physicians, it varies across the state. In the central part of the state, it's easily 100%. At the north, you know, in some parts of the state, it's as low as 50% of all the patients that a clinician is caring for.

Mike Klag - Johns Hopkins Bloomberg School of Public Health

Of those ten million who have given consent, how many require segmentation of their information and limitation?

Marc Overhage - Regenstrief - Director

As the exchange, we don't know the answer to how many people because that's a provider/patient decision, and so we don't know what data wasn't shared, and that's a good thing.

Mike Klag - Johns Hopkins Bloomberg School of Public Health

But I thought I heard you say that the information was sent centrally to the network, and then when the information ... when you got a request to limit it, then it was removed.

Marc Overhage - Regenstrief - Director

And I want to distinguish because I actually stumbled on my words a little bit there. There are two processes. One is when a provider and the patient decide that something shouldn't be shared, the provider does not make it available at all prospectively. There is also a process for a patient to, at any point say I don't want anybody at any time to see my information, and then that is the back office process.

Mike Klag - Johns Hopkins Bloomberg School of Public Health

If a field is blank, you don't know whether it's because it wasn't collected or....

Marc Overhage - Regenstrief - Director

That's correct.

Paul Egerman - eScription - CEO

Great. Thank you, Michael. Judy?

Judy Faulkner - Epic Systems - Founder

I asked this morning for someone to take a look at patients that we had who were asked by their healthcare organization if they wanted voluntarily to give prospective authorization to have their entire record go from one healthcare organization to another for purposes of treatment and care. So they counted 125,679 patients who were asked if they wanted to do that, and of that, 124,017 said yes, which is 98.7%. I think that's interesting.

Marc Overhage - Regenstrief - Director

...population...?

Judy Faulkner - Epic Systems - Founder

I think that was of the two groups that we looked at, the entire number of patients that they asked. So what I think is important is that I think the way that you were saying of doing it, Marc, which is the physician doesn't enter it in, or, if I understand it correctly, or if you enter it in, you mark it as a sensitive note, and that note doesn't get passed, are two ways that are reliable. But otherwise, so much is threaded.

If there's a disease they want to hide, what's threaded is it's in the diagnosis. It's in the problem list. It's in the medications. It's in the medication interactions. It's in the imaging. It's in the notes of the imaging professional. It's in the results. It's even in the order, so if you don't look at the results, you can tell by the orders, what the orders were looking for. It's in the group of physicians who are giving care. You can look at the backgrounds of the physicians and figure it out.

And so I think what is interesting is that it can be very misleading and unfair to the patient if they think that there is technology that can somehow go through and hide all that stuff because there's too much to hide. And it's too threaded. Then, secondly, of course, it compromises the quality of care.

What I think would be interesting if, for the purpose of ... we can separate out. I like that statement that it's not that the data shouldn't go, but that it shouldn't be improperly used. Could we not focus as much on what data goes because we ... the electronic systems need to recognize it's very, very difficult to effectively hide things. But should we instead be focusing on not penalizing the information that gets transferred, but penalizing if in fact it is inappropriately used.

Paul Egerman - eScripton - CEO

That's a good comment. Great.

Marc Overhage - Regenstrief - Director

Can I add one thing there, Paul?

Paul Egerman - eScripton - CEO

Sure.

Marc Overhage - Regenstrief - Director

Just one of the things just sort of on the ground pragmatic issues, so you talked about flagging fields or whatever. In reality, what most providers are able to do technologically today is if the patient chooses not to share some ... it is typically the whole encounter, whatever it is.

Judy Faulkner - Epic Systems - Founder

Agreed. Yes.

Marc Overhage - Regenstrief - Director

Everything about that hospitalization, that's typically what the providers are able to do today, so it....

Judy Faulkner - Epic Systems - Founder

But if that's a hospitalization, but if you're mixing all the ambulatory and inpatient together, it gets very threaded.

Marc Overhage - Regenstrief - Director

Right, so the data from that physician's encounter with the patient that day, as you say, the imaging study that's obtained later is a different challenge.

Paul Egerman - eScription - CEO

Great. Thank you.

Deborah Peel - Patient Privacy Rights - Founder & Chair

Well certainly the problem is inappropriate use of information, but the question is, who decides whether that use is inappropriate. Our organization and our coalition representing ten million Americans think that the one that should decide what use is inappropriate or not really is the individual. And there's no question that today many of the health IT systems don't have the ability to do granular kinds of blocking or segmenting data. That's today.

There are actually some systems like the NDIIC system that allows some pretty selective and detailed segmentation. Technically there is not going to be a problem eventually to get to being able to selectively eliminate every type of reference to a particular disorder. But you're certainly right if the person had faith that the information wouldn't be used against them, you know, then maybe that type of granularity would never be needed. And again, you know, that's the whole purpose that we're here and that we're delighted to have this opportunity to talk with you is because there's so much misuse of this very sensitive data. And unless the system is constructed to where the misuse that prevents jobs, prevents employment, prevents key opportunities in life are addressed, you know, this is going to be a no go, and we'll have no data.

Paul Egerman - eScription - CEO

Thank you. All set, Judy? Dr. Tang?

Paul Tang - Palo Alto Medical Foundation - VP & CMIO

Thanks for the panelists. It's been wonderful to hear the diverse range of opinions because it just helps inform the deliberations. A lot of the discussions in the past and a lot today have dealt with HIPAA and covered entities because we're saying data that comes from covered entities. In some sense, that's so 1996.

And to pick up on where Susannah talked about the ... going into these other places, a lot of which ... with the patient. And the question is voluntarily or involuntarily. So we have what seems innocuous, a PHR, a health risk assessment, social media, Facebook, etc., but there's a lot of confidential or private health information that gets shared, not necessarily understanding whether it's confidential or not, and clearly outside the realm of the protections of HIPAA and covered entities.

My question for you: The NHIN is thought of as a place where, and we gave in the meaningful use criteria, we wanted data to be an off ramp to the consumers. I think, in the future with the mobile and all these patient entered data, it'll also be an on ramp to the NHIN. Hence, the patient contributed data becomes part in the scope of what I think we need to deal with. My question for you is, do you think we have protections today for the patient entered data or patient contributed data into the health information ... and if not, what would you propose? Is it the – now just wait one second, Deven. Is it the granular consent on control that Deborah espouses, or is it that we need stricter rules that actually encompass the patient entered data and much along the lines of what Deven proposed, or is it somewhere in the middle?

Deborah Peel - Patient Privacy Rights - Founder & Chair

Frankly, we'd agree with both, and what you're bringing up is a really critical point. You don't have privacy or control unless you control sensitive health information wherever it is. And so the protections really have to follow the information, and Web sites that collect it and use it in surveys and so on are really misleading the public. Many of them use the data, the sensitive answers people give to health surveys to sell and to harm them with. And so, we need a system where it's recognized, like you're saying, covered entities and business associates are so 2009. This data is in many other places, and we believe most patients somewhat naively think that because they're going to a health related Web site,

those people are there to help them. So there has to be the ability to control the use of the data, and if I were to give my data to someone for a survey, it should be the purpose of providing me with the results of the survey. They shouldn't be able to then turn around and use it and sell it in other ways without consent.

Paul Tang - Palo Alto Medical Foundation - VP & CMIO

One interesting follow-up to that, and then I'd like to hear what Deven as to say, as well as the other panelists, but hasn't the consumer, since it is not coerced, they entered it themselves, implicitly then consented to everything? They clicked I agree to.

Deborah Peel - Patient Privacy Rights - Founder & Chair

No, they're totally not informed. I mean, you know this. When you go on a Web site, you can't even read those privacy policies. They're not informed. I mean, okay. Some people are getting savvy and understand that they can't trust whether it's Twitter or Facebook, who are now having to deal, by the way, with providing consumers with more control over their information because they found out how bad they are. But we don't have a way right now to understand even what the privacy policies are on most Web sites. It takes Deven's team of lawyers to tell us what the agreement actually says.

Deven McGraw - Center for Democracy & Technology - Director

Yes, and my fellow practitioners are the ones that write those damn things. I actually agree with Dr. Peel here. You need both. I mean, this is one of the areas where consumers ought to have a strong role in controlling their data. I mean, to some extent this is – and it should be voluntary whether they participate in them or not. And so, therefore, if they want to throw their data up on some Web site, it's not up to me to tell them they can't do that. But at a minimum, there ought to be, again, because I wouldn't want to pin it all on consent, consistent with my prior testimony. There ought to be some rules that govern even the Internet marketplace with respect to how they handle personal consumer data.

And this is actually something that we're working on here at CDT across all personal data and not just health data, and we've been working on it for many years. So I have folks that I work with, including a computer scientist who is the one who opens up the back of the computer and tells me what's actually going on, on particular sites and what they're doing and what data they're collecting, etc., which is incredibly helpful. But we have people working on consumer privacy as an overarching issue with respect to use of the Internet because we have no consumer privacy laws at the federal law to protect people when they use those, so there's sort of a lot of attention that needs to be paid here. It's definitely one of the gaps that we still need to fill. There's space to do that. There's a study that HHS needs to do in consultation with FTC to look at the PHR aspect of it, but just so that we're all aware, there's other activity going on that we should be mindful of an ideally in coordination with.

Paul Egerman - eScription - CEO

Susannah?

Susannah Fox - Pew Internet & American Life Project - Associate Director

Just to add a comment. I said we learn the hard way sometimes about how survey data doesn't really get to what people are actually going to do, and at one of the first health privacy conferences that I went to, I asked somebody who runs a really large Web site that helps people actually with cancer. And I asked, what's the privacy policy, and he said our policy is that you have no privacy....

Deborah Peel - Patient Privacy Rights - Founder & Chair

(Inaudible.)

Susannah Fox - Pew Internet & American Life Project - Associate Director

Yes, because it was – it was ... Friedman of Acore.

Deborah Peel - Patient Privacy Rights - Founder & Chair

(Inaudible.)

Susannah Fox - Pew Internet & American Life Project - Associate Director

So essentially when people are facing death, they are willing to give up their information, and this is what we're talking about. So it is coerced, or is it just practical that they're willing to say, here are my symptoms. Does anybody else have this? What is the protocol that helped you? And I think that you actually have a great opportunity to look at what else is happening in terms of adoption and behavior online. Learn from what Facebook learned. Look at what Twitter is working out, frankly, this week in terms of who has control over what you say and do online, and look at what consumers, how consumers are benefitting.

We have consistently asked questions about whether people have found benefits in the health information they find online. That is growing. We've asked whether there's been harm. That is a flatliner. So people are really getting quite a bit of benefit from social media, from being able to search for health information to gather and share it online. Please look at that and understand that you have lots of other industries to look besides health care, which is, frankly way behind the curve.

Speaker

I'd like to make one little comment about that, which is that people regard the Internet in a sense as a health provider now. They're seeking health information. One thing that's different about privacy for Twitter and Facebook is that Americans have the strongest rights of control over personal health information of any information that exists about them. In other venues, we don't have a long history of the right to control personal information. So that's somewhat different than in commercial venues and that's why people are getting so concerned. So it's important to understand that really people are looking to the Internet and to social media for help in the same way that they would turn to other providers. So I think it's pretty logical to think that those other providers also owe them the same kind of duty and respect not to misuse their information.

David Blumenthal - Department of HHS - National Coordinator for Health IT

Thank you.

Marc Overhage - Regenstrief - Director

I had two quick comments. I promise that they're quick and then a question that's also quick. First I'm worried about absolutes and things like consent because I think surveillance, disease surveillance, there shouldn't need to be a consent. That's public health, that's public safety. And so there are going to be things where I don't think I line up completely with absolutes around consent.

The second one is around technology and implementation of it. The only times I hear the terms cheap and simple are when they're talking about me. It doesn't matter where we're at today. I still have people that mess up with their faxing machine and send the wrong information. So it is a very difficult thing around the technology enablement itself.

And then I guess the question I have is I've heard a lot of the statistics that are out there. Has anyone done any surveys that would align the costs associated with privacy and their willingness to adopt to that level of privacy? Because I think we do a pretty good job with the requirements that are out there today, at least I think we do as an organization personally. And that this incremental increase has a lot of cost associated with it. Has anyone done that level of surveying?

Paul Eggerman - eScription - CEO

I have a response to all of this, of course. The first thing about public health is, yes, the public endorses public health. But if you look at what public health collects, the information it collects over the history of the development of the field of public health, it's pretty much been by statute. It started out with dangerous and infectious diseases, the collection of data, TB, various kinds of frightening infectious

diseases, but typically the data collection has been what's being collected and how it's going to be handled has been argued in legislatures with public debate. There's not a broad mandate for public health to decide what it wants to do, which is something of the direction taken by the commissioner in New York. But up until the present time, public health has been what data is collected for the good of all has been argued and debated with the good of all. So we're not opposed to public health, we're very much for public debate about uses of information, particularly population based uses of information.

So, yes, I sound really absolute and it's because I'm a practicing physician and I've seen the absolutes that happen when people don't have control. HHS' own figures indicate that 600,000 people a year don't seek early diagnosis or treatment for cancer because they're afraid they can't control the information. Another two million don't seek treatment or help for mental health because they think it won't remain private and so there are real costs to not paying to do this right up front. We could blow the system, we could never get the trust back, the public's trust is we'd lose it because we don't do it right in the first place. There's real costs to not having privacy, bad outcomes, people getting delayed care, people losing their lives. Bad outcomes are a real cost of no privacy.

Speaker

Mark, there are some studies, maybe none that have done that I'm aware of of new provisions. But a couple that come out that, of course, Deb and I take turns punching holes in. I've never seen anything. There's studies that what are the costs of privacy. There was one that came out fairly recently about what are the costs of state laws in particular that require consents for particular pieces of data. One that's sitting in my email inbox waiting for me to read it that I just got this week that yet, again, raises this issue of cost, I've yet to see a single one that also took into account the costs of not doing anything in terms of the damage to people's trust. So ideally, we could put it all on the table and think about what are the incremental costs of these more onerous, potentially more onerous, we've haven't worked all this stuff out yet, right, requirements on providers versus what are the costs of not doing that. I've yet to see anything like that, but there's certainly are studies out there about cost.

Speaker

Well, there's also the experience of the U.K. They spent hundreds of millions or billions on a system and they've had to go back to reengineer consent in up front. So there's experience around the world to look at it in terms of cost and blowing trust.

Michael Weiner, CMO, Defense Health Information Management System

I would just add that what Mark said I think about in addition to public health, safety and looking at quality care, that information needs to be included for all patients, not all data, but the important indicators. But to get back to the informed consent issue, it just seems to me that it's a conundrum that because as complexity of the consent information increases, understanding goes down. We've seen this with research consent where we work very hard to have a ninth grade reading level. We had people, it's culturally understandable. And then we have a 12 page boilerplate on the back of it that meets federal regs. So we don't believe that patients understand that 12 pages, but our general counsel says you must do this.

So I hear a push from Dr. Peal to say you, Paul, called granularity, but very specific information, which means it gets longer. Even if you have a physician involved or a health care provider involved, it gets so complex, people can't understand it. So how do we solve this issue of empowering patients, giving patients control, but understanding that the consent process take time? And it's complex enough to cover the kind of things we're talking about here, very few people will understand it.

Speaker

I really hope that you will convene a panel with some of the innovators in consents, so that you can see how consents can be interactive and intuitive. There's one particular company that we've talked about and we've put on a list to you that works with a group of victims and families with a genetic problem. They show examples from their own group of different consent choices people have made and why. There are ways that this can be done in a much more visual interactive drop down kind of way. There's beautiful ways that technology can help.

Speaker

Is that consent for care or for research?

Speaker

The section that I've been thinking about is about research, but it involves segmenting versus sharing different pieces of information. It walks people through things. Or even, for example, I think we're going to find consumers are going to get more sophisticated about consent. I don't know about your kids, but my kids are learning about consent management systems from Facebook. You're in, you're out.

And then if you look at, for example, Microsoft Health Vault, they have various partners and before data is shared, the partner, let's say Pulse Watches, because you want to figure out how good is my heart rate doing on my workout. If you want to get information from Pulse through Microsoft, you get to share only the data that's relevant to Pulse company telling you how you compare to yourself and to other people that are you age and weight and so forth. So there are mechanisms out there that are beginning to teach people the concept of, you don't have to share everything to get a certain kind of help that you want. I think we're actually farther along in developing consent mechanisms that the committee may be aware of.

Paul Egerman - eScription - CEO

We only have a couple minutes left. I know Mark has a comment, so go ahead, Mark.

Marc Overhage - Regenstrief - Director

...you talked about the clinician being—just to share a specific anecdote, this was within the need of greater delivery system, but I got involved because of some of ... But a physician ordered an MRI on themselves and the result was returned to the physician's practice as is the usual protocol and he was very upset with the health care system that the results went back to his practice and it was available to the people in his practice. You would think of all people who might be able to understand the implication, but this is the person who is supposed to be helping educate patients. And to Evan's point, I think it's a challenge even for attorney's and physicians who do this day in, day out, even harder for the patient who has to deal with the health care system in difficult and stressful circumstances.

Paul Egerman - eScription - CEO

We have about one minute left, so you'll have to be very brief, Christine.

Connie Delaney, Dean, University of Minnesota School of Nursing

Connie Delaney, and I'd like an opportunity to speak as a member of the committee. Thank you very much for recognizing my opportunity to speak and I will be consistently available via phone today. I wanted to comment on several points. First of all, I'd like to reinforce Gail's comment early on in the committee comment opportunity that reflected on our commitment and our responsibility to the consumer focus and being attentive, responsive, and I would hope deeply exploratory on how we continue to empower the consumer to have very much a shared responsibility and accountability in this area of privacy, as well as sharing data.

Second, I would like to make a comment on, Mark, your presentation and your responses to questions. I want to particularly support the auditoria mechanism that you summarized, Mark. I know that is just a very high level summarization. The opportunity for this committee to consider the wisdom and the support of audit trail requirements in the deliberations and final recommendations of this committee. That also then includes and can include as Mark summarized the strong emphasis on the authentication requirements.

My last comment relates to I believe that as a committee, we have an opportunity to forward recommendations ultimately that actually don't accept a lot of the, if you will, lower bar that we're operating under. I believe we have an opportunity and I would certainly support the deliberations that would support truly raising the bar related to the privacy issue. I say that because I am deeply committed as I know all of us are that unless we can support the growth and ongoing trust of the American public in the work that we're trying to advance, whether it's sooner or later, ultimately our efforts will depend on that level of trust that we can support. Thank you for allowing me to make these comments.

Paul Egerman - eScripton - CEO

Thank you very much, Connie. I think we're out of time. I'm sure Dr. Blumenthal is about say this, but I want to say thank you very much to the four panelists for an interesting and spirited discussion.

David Blumenthal, National Coordinator for Health IT, Department of HHS

Yes, I agree. This has been very educational, I'm sure, to many of us and opened up some new specters. We have to avoid being very 2009 in our thinking. Though, maybe there are some things from the past that we might not want to forget as well.

We have a 15 minute break scheduled. I know we're going to be losing some people on the early side. But I think it's a lot to ask people to sit for three and a half hours without an opportunity to stretch their legs. So rather than a 15 minute break, what I'm going to suggest is we take a five minute break and come back here, five minutes of.

Deven McGraw is earning a lot of credits for this particular meeting, having been thrown into the breach because of John Roberts' absence and...providing testimony, she's now being called upon to moderate one of these sessions. So she's seeing it from sides. I want to thank our panelists. I know that one of our panelists, I think, has to leave at noon, but we should be finished by then with Deven's expert moderating. So at this point, I'm going to turn the gavel I wish I had over to Deven.

Deven McGraw, Director, Center for Democracy & Technology

You did pretty well with the pen and the glass. This panel is covering the topics of the use, disclosure, secondary uses and data stewardship. Our first presenter is Eileen Twiggs who is the National Director of Information Systems and Technology at Planner Parenthood Federation of America. Eileen, go ahead.

Eileen Twiggs - National Director of Information Systems & Technology - Planned Parenthood Federation of America

Thanks, Deven, good morning. Thank you for the opportunity to provide testimony to the HIT Policy committee. Planned Parenthood Federation of America is a national not for profit organization. We provide services to 93 separately incorporated affiliates. Our affiliates operate more than 850 reproductive health care centers in almost every state. Each year Planned Parenthood health centers provide reproductive health care, including routine gyn exams, breast and cervical cancer screens, contraceptive services, abortion care, STI testing and treatment and HIV testing and education. Planned Parenthood sees more than three million patients each year and the vast majority of our patients are low income. And for most of them, we are their sole provider.

Planned Parenthood brings to bear more than 90 years of experience providing highly sensitive, confidential health care. We understand the value that technology brings to health care and we already have a national initiative underway to standardize our own clinical information systems. The consideration of privacy and security issues in the context of the care that Planned Parenthood provides will test the boundaries of the health information exchange debate. Yet our patients deserve the benefits that will come from health information exchange.

For this reason, we are moving forward with the understanding that sensitive data will be part of the exchange. However, in order to include sensitive data, a comprehensive privacy and security framework must be developed. We appreciate that this will be a complex undertaking, one that must include specific situational analysis to insure that all risks, especially those for the most sensitive information are appropriately addressed. In Planned Parenthood's world, there are individual, organizational and societal considerations for privacy and security.

First, patients often come to Planned Parenthood specifically to insure that their family, insurer, employer, or other health care providers do not know that they have obtained our care. Second, our providers risk their personal safety by coming to work every day and doing their jobs. Finally, Planned Parenthood is frequently targeted by organizations and individuals, including government officials, who want patient information to further a political agenda.

Consider a 30 year old woman who is in an abusive marriage. She's previously received treatment at Planned Parenthood. It could be for birth control, treatment of an infection, or an abortion. Whatever it is, she doesn't want her husband to know. Now her husband brings her to the emergency room at her local community hospital with an elevated heart rate. The emergency room clinician is an anti-choice activist and she has access to the health information exchange. This could mean access to the patient's complete medical history and to the name of the Planned Parenthood provider.

Who determines what information is legitimately needed? How can we insure that specific information will not be made known to her husband? How do we prevent the misuse of health information, be it at the expense of the patient or the provider? The stakes are definitely high. Stigma accompanies reproductive health care. The release of confidential information may compromise the patients and the providers' personal safety. It could lead to acts of discrimination and patients may delay or avoid seeking care if they believe their privacy will be compromised.

As you can see, we have a unique role in the continuum of care. We know there are no simple solutions. We're still working through these issues ourselves. But while there's much to decide, we strongly believe that there are five critical principles.

First, we must protect the original understanding developed between the patient and the provider. In other words, we have to honor the contract. This mean decision making authority over the release of health information must remain at the point of care with the patient and the provider. Providers must retain the same level of professional judgment in an electronic environment that they have in a more traditional environment.

Second, participants in the exchange should only access the information necessary to meet the needs that they have and to serve the patient. We can call this the less is more principle. To accomplish this, policies will also need to appropriately tailor the scope of the information exchanges to the role of the party requesting it.

Third, policies must define a participant's responsibility with respect to health information after it is exchanged. In other words once confidential, always confidential. Clear standards must be developed to clarify the obligations for all types of participants. We have to pay special attention to the use of sensitive information. Patients will expect that their information will remain confidential wherever it goes.

Fourth, inappropriate access must be denied. Simply put, there can be no prying eyes. This applies both within the continuum of care and outside. Those without a legitimate right for access, whether they're medical professionals or family members, employers, insurers, or politicians must remain at bay.

Lastly, we must proactively detect, report and penalize noncompliance. In short accountability is essential. Privacy and security violations should have substantial consequences and penalties should be commensurate to the nature of the misuse. This should include heightened civil and criminal liability and professional sanctions for the misuse of sensitive information.

To achieve the real goals of health information exchange, everyone must participate. This is only possible if patients trust and have confidence in the privacy and security of the system. Most of our patients already face significant challenges. They can't be denied access to the benefits promised by health information exchange. We are ready to work with this committee, so that all necessary protections can be developed.

Again, we thank you for the opportunity to contribute to the national conversation on these important issues.

Deven McGraw, Director, Center for Democracy & Technology

Thank you very much, Eileen. The next presenter is John Houston. Dr. Houston is the Vice President Privacy and Information Security, Assistant Counsel and Adjunct Assistant professor of biomedical informatics at the University of Pittsburgh School of Medicine and a member of the National Committee on Vital and Health Statistics.

Dr. John Houston – University of Pittsburgh Medical Center.

You do have my testimony, so I'm just to go over a couple of highlights of it. Also I want to call attention to two reports that NCVH does put out, one on privacy and confidentiality specifically related to NHIN and sensitive information, as well as another report on data stewardship have a lot of recommendations in them. So I'm not going to really touch too much on those two reports, but I really think they are outstanding reports and encompasses a lot of testimony and a lot of deliberation over a number of years and includes input from people like Paul and others. So I think it's really good for you guys, if you want to get a good understanding of what some of the issues are.

As a privacy and security officer and due to my involvement in NCHS, I'm really am very sensitive to privacy and security. But I'm also very sensitive, I have to be pragmatic about the realities of trying to deliver health care. So a lot of what I'm going to say today is based upon that balance.

The problem that I see with privacy is that privacy is a societal value. Each and every one of us in good faith has a difference of opinion as to what privacy is and what it means to them. These opinions vary dramatically. When I hear testimony, you hear somebody from one end of the spectrum and then somebody from the other end of the spectrum and you're both right. So it's difficult to try to balance that. At the same time privacy is not something that's quantifiable. If we try to put in place criteria X, Y and Z and ask people to comply with them or organizations to comply with them, does that organization have privacy? And the reality is it may or it may not.

So I think one of the dilemmas that I see in trying to from a meaningful use perspective and overall is it's how do you develop criteria that organizations comply with and at the end of the day, you can say they have privacy? Unfortunately, I don't think that exists. So as such, I think my advice is, we need to try to do the best job that we can with HIPAA and with ARRA and then really try to enforce both and put good enforcement mechanisms in place that are not overly prescriptive or they're not arbitrary and we just have to figure out a way for them to be effective.

Regarding security, I think we have to make sure that whatever we put in place is flexible. New technologies evolve. New threats emerge daily. Provider operations vary dramatically. So as we're trying to develop criteria as what type of security needs to be in place, we need to make sure that we're flexible. Otherwise what I think we're going to end up doing is, we're going to stifle innovation and we're

going to have problems trying to define meaningful use in a way that people can comply with while trying to deploy information systems in a meaningful way.

With regards to data exchanges and in HIN and in the context of use and disclosure and data stewardship, in addition to all the recommendations that NCVHS has made, I really think that it is absolutely vital and it's to Dr. Blumenthal's point this morning that we have to have some type of oversight process at the macro level. I believe that that there really needs to be a central organization that coordinates, polices, acts as anregarding privacy and security. There has to be an organization in place that do anything from credentialing participating providers, so that you can't even get into the network unless you have met some very stringent criteria and that you make some very strong—that you enter into agreements with some very strong criteria as to how you're going to act.

We also need to provide a mechanism to allow patients to see where their information has been disclosed. The idea of consents, I've heard a lot of discussion about whether they're meaningful or not. But one of the strongest vehicles for insuring that people do the right thing is often allowing the patients to see where their information has actually been sent to and who has seen it. So having a way for a patient to see where their information has gone and who's looked at it, I think is very important.

Now ARRA provides for that at the covered entity level. But we start to pass information across the United States, I think it's going to become much more important and it's going to be much more difficult to make sure the patients also understand where that information has gone often very transparently and with very few restrictions.

Thirdly, I think that this organization needs to be able to investigate inappropriate disclosures when a covered entity may have done something bad. How do you police it? I think an organization has to be in place to do that.

And then fourthly, I think that if patients can limit what information can be sent where, if we allow them to decide that sensitive information can be restricted from disclosure, we have to provide a vehicle for patients to conveniently decide what they do and don't want passed across this network.

So in the end, I think it's critical that we get this right. To get it wrong will in some form result in patient harm. Too much access to data or too little access to data can cause very similar harms in the end. Unfortunately, this is not a topic that lends itself well to straight forward and simple solutions. So I've been dealing with this, wrestling with this for seven years on NCVHS and had a lot of debate and lot of dialog on these topic and it ain't easy. But we do have to get it right, so thank you.

Deven McGraw, Director, Center for Democracy & Technology

Thanks a lot, John. I really appreciate it. Our last presenter is Jim Golden. Dr. Golden is the Director of the Minnesota Department of Health Division of Health Policy. He's been designated by the governor as the state government health IT coordinator. Jim, we apologize that we didn't have a name tag for you, but now we all know who you are, so go right ahead.

Dr. James Golden – Minnesota Department of Health

Good morning and thank you for holding this meeting and allowing me participate on the use, disclosure and secondary uses of health information, specifically as it relates to public health. I'm representing the Minnesota e-Health Initiative, which is a public/private collaboration whose vision is to accelerate the adoption and use of health information technologies and electronic health records in particular. This initiative is guided by a legislatively chartered state advisory committee with 25 representatives that broadly represent stakeholder groups with an interest in electronic health records and has included public health from the beginning.

Public health is concerned with threats to the overall health of the community, based on the ongoing analysis of the population's health. Governmental public health agencies provide the backbone to the public health infrastructure. But this infrastructure is also dependent on other entities, such as physicians, clinics, hospitals and others in the health care delivery system. It's also dependent on the public health

and health science academia at universities, social services and others engaged in health related activities. It's critical that these entities are able to exchange information.

Public health has a long history of implementing appropriate privacy and security measures to protect information that's been collected for public health purposes. One of the reasons that they have such a long history is because public health practice often requires the acquisition, use and exchange of individually identified health information in order to perform the essential public health activities, including disease surveillance, outbreak investigation, the delivery of direct health services and public health research. Such information is necessary for public health authorities to implement mandated activities and to accomplish our public health objectives.

Health information exchange presents a tremendous opportunity for public health to prevent disease, both infectious and chronic using cutting edge technologies. In my notes I had 21st century, but given that we were previously arguing in the last one about 2009, 2011 and 1996, I think I'll just stay with cutting edge technologies and methods. A comprehensive reformed health system in America needs to control costs, expand access and improve the quality of care, but it also needs to focus on the well being and public health will be critical to that focus as well. As you consider public health's role in health information exchange, let me just share a few things to help keep in mind.

First, the detailed frameworks for protecting the privacy of health information for public health activities have been usually extensively discussed and debated in state legislatures and try to reflect a balance of different stakeholder concerns. During the course of developing those frameworks and policies, there are many mechanisms for different stakeholders to provide their input and to try to compromise and find balance between the different interests that are getting represented.

While in some cases, federal solutions may be appropriate to meeting the needs of stakeholders, states need to continue to have a lead role in setting and developing public health policy. Public health activities are based in communities and states are more closely connected to the local communities and able to reflect their different values and desires of the stakeholders who are involved. Currently public health frameworks are not uniform and may not be simple. I'll come back to that in a second.

In thinking about the development of the framework for the national health information network, we would just ask that you keep four things in mind. One, public health has a critical role in protecting the community. Number two, public health often requires and is needing to get individually identified data in order to appropriately protect the public health and improve the health of the population. Three, the privacy and security frameworks for public health reflect the stakeholder interest and the perceptions about the public health threat, the needs and abilities of stakeholders to participate in information related to those threats and the balance of public health goals with other important public policy goals. And four, that there is tremendous difference between local and state policies. And these are often reflective of variations in stakeholders' values and interests.

So in thinking about the complexity and lack of uniformity in public health privacy frameworks, what would I say? If you look at them one by one, it's kind of looking at a forest and trying to look at the trees and vines and make something out of it. It's very difficult. But when you start to look at it as a forest, you can start to see a wide variety of common things that apply to all of these. And so thinking about the elements that apply to these frameworks, I would simply say, some of the characteristics would include trying to define the ability of the individuals to participate in decisions to collect, use or disclose identifiable data. That might include consent in, it might include the ability to opt out or it might include the ability not to have any consent at all. There's a variety of information that needs to be provided to the individual as well.

Second, the ability of an individual to know how and when their identifiable information has been used or disclosed. This may require auditing functions and it may require notifications. The ability of an individual to access and amend their individually identifiable information, this may include the ability of an individual to access their information and a mechanism to challenge the accuracy; the ability of an individual to

challenge the compliance with legal and privacy frameworks; the need to maintain role based access to data; and the need potentially to have time limited access or disclosure of data.

In conclusion, public health is an integral component of the comprehensive vision of e-health in Minnesota and the nation. We believe that including population health and public health in our e-health framework is essential to achieving the effective use of health information technologies. And public health should be included at an achievable level in the initial definitions of meaningful use. How public health needs are included in the concept of meaningful use should increase over time as systems are modernized and capacities for exchange increase. Thank you.

Deven McGraw, Director, Center for Democracy & Technology

Thanks a lot. I appreciate it, Dr. Golden. We'll now move into the period of questions from committee members. Go ahead, Charles.

Charles Kennedy – WellPoint, Inc.

A comment and a question. I didn't get this in at the last panel. I'll make this brief. There was a statement made that health plans share data with employer groups with an implication that that was inappropriate. In fact under HIPAA, when an employer group is self insured, the employer group as a covered entity, we are the business associates. So it's not that we're sharing data in an inappropriate way. We're simply following the law.

That aside, second point, I was really struck by Eileen's example of a presumably dysfunctional relationship and information coming out inappropriately. I was recalling back to Judy's comments about threads, about how data within records is so threaded, that you can pretty much figure out what's going on even if certain pieces of information are hid. So my question to the panel is, if self systems can do a better job at separating a diabetes thread from a manic depressive thread, aren't we essentially stuck with an all in or all out kind of situation? Or do you think there's ways we could begin to have a finer granularity of privacy in the near term?

Paul Egerman - eScription - CEO

It's a great question. I'm dealing with this all the time within a large health system. Unfortunately, no matter how much you would like to say medicine is a science, it's also an art. I hear time and again from physicians where they want information, they need information. So often information that might be part of psych encounter, drugs, medications, lab tests may have meaning even in other contexts. What medications a patient is on—if a patient is rolled into an emergency department unconscious, the physician needs to know. If a hospital has a psych unit, say, for instance, you might have people that from an emergency department or intensiveness because of a codes condition, have to go treat a patient on one of those psych units. And if they don't have access to the psych data, there could be catastrophic consequences.

So trying understand exactly what information is necessary at any given time in order to provide treatment, it's very difficult. So you almost have to err on the side of more information, but more accountability by these individuals, so that they do the right thing. And you have to have some way to enforce or some way to be able to retrospectively monitor because you can't necessarily prospectively restrict. But it is definitely a balance in one, as I said, I struggle with it constantly as a privacy officer. I have had meetings with seven, eight physicians, as well as other individuals from a privacy perspective, talking about how are we going to do this, what can we do because the lack of information can be deadly.

I don't know if that's a good answer or not, but it is one that we are challenged with all the time.

Deven McGraw, Director, Center for Democracy & Technology

Eileen, did you want to answer that?

Eileen Twiggs - National Director of Information Systems & Technology - Planner Parenthood Federation of America

I would agree with that completely. I think the issue of accountability here and of having clear understandings and transparency within the exchange community, as well as outside of it as to when information can be accessed and for what purposes is going to be key in making this successful, particularly while we're waiting for technology to evolve where we can get down to a more granular level of protection.

If we don't have a common understanding about what's appropriate to be releases and for what purposes, the risks to the patient community are just too high.

Speaker

Thank you.

Deven McGraw, Director, Center for Democracy & Technology

Gayle.

Gayle Harrell – Former Florida State Legislature

I'd like to ask another question down another line. We were considering what are the best ways to handle things. Not only do we have consent, but also documentation and audit trails of who accesses information. But let's think about the patient's perspective and go back to the basics of what the patient wants to know as well. Give me your opinions on what your thoughts are notification of patients when information is actually accessed. Do you have any thoughts on perhaps that as a mechanism of really putting controls in the system when you empower the patient to know that that information has been passed, not just a request documentation later on to follow an audit trail after something has happened, but perhaps up front to being notified if my information is being passed to another entity with or without consent.

Eileen Twiggs - National Director of Information Systems & Technology - Planner Parenthood Federation of America

So I think patients definitely have a right to know when their information is being used and for what purposes. My concern lies in getting the balance of that information, so that it's meaningful. So in other words, if my expectation as a patient when I come in for care is that you're going to give my information to my insurer to get my bill paid, I may not need to know that that use in particular has been made, when it's been made if there was a question that came back in a rerelease and a clarification of information. Oftentimes there will just be a level of back and forth between a provider and an insurer in terms of claims management that may be overwhelming to a patient if they're actually notified every single time a different piece of information is released.

However, when information is released for purposes that a patient is not expecting, then I think that that would be an appropriate circumstance to have patient notification. We want to manage the level of information, so that when it comes into the patient, it's meaningful, so that they don't just say, oh, I'm getting another beep from the health information exchange that someone else has my information. And it just almost becomes meaningless.

So I think unfortunately there really are no simple solutions and with any number of things, this is going to be a bit of a balancing act.

Speaker

I think in the case of public health, we often require mandatory reporting for a variety of infectious diseases. I think that there are a wide variety of ways that a citizen in the state could understand that. We make that information available. We identify when we collect information without the patient's consent that's maybe mandatory from an organization. When we collect information directly from the individual, we are required to tell the individual if they have a legal obligation to provide the intended use

of that information, the ability to use or further disclose the information beyond the intended use. The benefits and risks of supplying the data and the consequences of not supplying the data. So we do try to tell individuals with that up front in a meaningful way. So I'm not sure if it would be helpful if every time we used it or further disclosed it beyond those activities for the patient to get that information.

The other thing I would say on behalf of the e-health initiative is that in talking with a number of large integrated systems, you're asking specifically, I think, about disclosures. But if you think about uses, one of the concerns that a large system has within their facility about who might have used or accessed the data is that if you're in a hospital, you might see four or five care providers, but there might be a legitimate reason for 40 or 50 individuals to have to that data. I think the general belief of many in our health community, particularly in a hospital would be that that information would be very disconcerting to a patient, confusing because they may not understand all of the business operations within such an entity and it may not add, actually, protecting or even clarifying anything for those patients.

Marc Overhage - Regenstrief - Director

Let me add actually I read a study where these complexes cases, more than 40 or 50, it can be up to 200 people who might have access. So at a macro level, I think it is very important that there be some level of transparency. So a patient sees where their information is being disclosed. If they were never in Washington DC and provider in Washington DC asks for their records, they might question why that occurred. The same thing is if they suspect that their neighbor looked at their record and their neighbor happens to work for a hospital and are able to go to the provider and say specifically did this individual look at my record, that can be meaningful as well. Looking at the whole list of 200 people may or may not if they know who they're looking for, but it can also cause a lot of distress for the patient and can actually be a lot of work that I think has no meaning.

Now having said that, one of the things that my health system does and we're very aggressive about is every user of our systems, their manager has to request their access. And their manager also has an obligation, we send them logs every day and alerts every day. And the manager is responsible for reviewing an individual's access. We do certain, other types of reports, such as same last name searches to see if somebody looked at a family member's record, which is inappropriate. We also VIP reports as well. If any of those trigger occur, the manager has to go back and ask the employee why.

So as we continue to make these more sophisticated, these reports more sophisticated, we're going to catch a lot of that activity ourselves. I think that is really important because alternatively what happens is is that the employees become more sensitive to the fact that if they look at something, they're going to get caught and it's going to cut down on people's willingness or desire to do just that. So there's a lot of different things we can do, there's a lot of balances, too, because you can run down a road and have an enormous amount of data that has no meaning to it.

Deven McGraw, Director, Center for Democracy & Technology

Thank you, all. I now have quite the list, five folks on here. So with Paul, David, Adam, Neil, Jim and then we'll go from there, so go ahead, Paul.

Paul Tang, Internist, VP & CMIO, Palo Alto Medical Foundation

Just a warning, I'm going to put the panel on the spot. So we heard about the importance of public health information, but keep it local. We've heard about the not too much and not too little approach and we've heard about respecting the covenant that the provider has with the patient and all of those are as a previous panelist said, motherhood and apple pie. But they are all very, very important. We've reused the work balance an awful lot. The NCVHS report, which is a really good basis for a lot of our deliberations talked a lot about the key issues and the pro's and the con's and spoke to balance.

So the spot comes in terms of let's get down to what Gayle says of practicality and somewhere along the line, we have to take the next step and go towards a solution or at least start making actions to reconcile these things because data is going to start exchanging. Let me put it into three lumps. One is we could put the burden on the patient as Deven was saying in terms of make it a consent. Another might be the trust to verify and in a sense, that puts the burden on the provider with the audit log. A third might be putting the burden on the regulator or the legislature, saying here are the rules that everybody has to comply with.

So I'm going to preempt and say you can't say, well,of all. But where would you put, if not all your eggs in one basket, where would you put the majority of your eggs in that continuum just as a start of a direction of where we might start talking?

Marc Overhage - Regenstrief - Director

Nobody wants to answer your question. I will start. I think absent a corrective consent can be something that patients, they simply sign and it's very difficult to get meaningful consent for things. I don't think regulations is necessarily a good thing either in terms of having regulators come and visit your facility all the time. I think that that can be actually getting in the way of trying to deliver quality health. I think the middle one, trust and verify, I think if I'm getting this correct is really the way we have to go. I think between internally reviewing access and the way people are accessing information, as well as providing this transparency to the patient can see who's looked at what, where information has been sent, I think those two things, I think, cause the system to achieve a reasonable balance. And we're still need to have regulation. Obviously and regulators come and if there's issues and there still needs to be some level of consent, especially for sensitive information. But these other controls, I think, can act and mitigate and work nicely.

Speaker

Mr. Chair, I think that's a false choice that you've given us. I think the reason is, I know you said don't say all of them, but the reason that I think it's a false choice is I do think that there is a need for some of these and let me give you an example. In the case of infectious disease, my experience in dealing with consumers is that they understand that they might get that through no fault of their own. They are very much less concerned about data being moved for their protection with infectious diseases. When you start to get into chronic disease, they view that more as a lifestyle choice and there they want much more control over how their information goes. So I really believe that you have to develop a system that can accommodate different levels of responsibility for different purposes, different roles and different types of information.

So I think that the system has to be sophisticated enough over time to be able to accomplish the different options that you provided. I think the one area where I really agree with John the most is it's very, very difficult to do this very accurately prospectively. I think the real key is to find ways to incent all of the actors in the exchange, whether it's the requester, the discloser, or someone else that exchange mechanism to act appropriately. There might be a wide variety of ways, it might be social norms, it might be a legal structure. In Minnesota in the private industry, we have a private right of action for the inappropriate use of health information. And we haven't found this caused us a big legal problem, but it does cause our providers to think much more carefully about how they use information.

Speaker

The only thing that I would add is that I feel that there is a new player here that we haven't really considered in your three choices, which is the role of the exchange. So while I don't think that the exchange has a role to play necessarily in deciding when and how information gets released. I do think

that the exchange has an enormous role to play in detecting and enforcing the community norms, however they're established. And so I would say that we need to actually put a large role in terms of accountability measures and monitoring and enforcement at the exchange level, so that they can actually understand how the community as a whole is acting, as opposed to leaving it with each provider to police themselves and their neighbors.

Deven McGraw, Director, Center for Democracy & Technology

Before we move to David Lansky who's next on my list, I will say as a process point, you are all invited, unless a question is directed to one of you specifically, of course, any of you can comment, but you shouldn't feel obligated to so to each and every question. I'm not suggesting that you have, but I looking at my list here. We have a shorter amount of time for this particular panel in trying to manage it appropriately. So go ahead, David.

David Lansky - President & CEO - Pacific Business Group on Health

My thinking is following the same lines, I think, as Paul's. I'm trying to structure this in my mind a little bit and I'm thinking I have three also buckets, three different ones. We can classify the data as sensitive, to varying degrees of sensitivity. We can classify and qualify users. We can manage transactions between them. And each of those three levels can have some technical tools brought to bear. I'm interested in two particularly that used to be talked about, but I don't hear much now maybe for good reason and we can take them off the table or not.

One was, I think, National Health Service had for a time, I don't know how they ended up implementing this. Hopefully, someone does. They contemplated that they called an envelope, which was a notion of putting sensitive or declared data by the consumer, saying this call of data for me is sensitive. I would like for it to be treated offline, in effect, in an envelope, which is only available for certain users and situations. It must then be auditable as having been accessed separately. So there's a cutting across these three levels I'm talking about. I don't know if the NHS pursued that or what is happened technically to implementing it, but it'sexperiment with that kind of solution.

The second similar idea is what we used to talk about is break glass, which is essentially have a class of users who would be permitted access to sensitive data in emergency room situations I think that John described. But that also would be revealed and audited promptly, so that the appropriate...would be inspected. If there are sanctions associated with inappropriate use as in the case of some of the reproductive health issues we were talking about, those could be made manifest.

So with those two solutions, so to speak, that would seem related on the table and are the relevant to the discussion we're having?

Speaker

I think they're absolutely on the table. I think part of the issue that needs to be discussed and decided is the levels of, so for instance, in the envelope or the break glass, and I honestly view them very similarly as to what the scope of the authority around how that information gets used, who that authority lies with. Because right now, HIPAA actually allocates responsibility for how information is used largely between the provider and the patient. This was something that the earlier panel discussed.

In giving a patient the authority to remove their information from the exchange altogether, maybe with the exception of a break the glass emergency scenario, actually may not be in the interests of fostering patient safety and quality assurance and public health activities. And so I think that there needs to be a clear understanding at the outset by both the patient and the provider as to the types of uses that will be made and there needs to be trust that those uses will be made in accordance with the framework that's been developed and the understandings that the patient and the provider have.

So I think they're both on the table, but I don't think that they alleviate the need to actually still have roles based permissions and transactional based scope and limitations.

Marc Overhage - Regenstrief - Director

I think that they're all incomplete solutions to some degree. I think break the glass is a good concept and I think to some degree, I think it's important to have that functionality. But there's a whole class of information that I hear when talking to physicians that they always need to have access to. It might be part of the sensitive encounter that you want to hide behind the glass. But medications and lab tests, some of them don't have any direct relationship to a particular sensitive encounter, but they're of meaning to that physician. Even something like methadone might have multiple uses. But always when you're prescribing medications, you need to know what other medications the patient has been prescribed, so in one context how much information is hid behind the glass and making sure you get that right.

The second thing is, is if you know that there's a glass there that can be broken, how do you know whether it's meaningful or not. Is there something there that I need to break it to see anything or do you put more context to it? Is the psych data there? Is there drug and alcohol treatment data there? Is there treatment related to a therapeutic abortion? How does the physician even know when to break the glass and what's relevant? It could be that somebody decides that sensitive information is the fact that they had cosmetic surgery. Maybe there's never any relevance to the fact that that person has recovered from the surgery. That the fact that that occurred.

That's the dilemmas and I think that in concept breaking the glass makes sense, but it's not the end all, be all to do you try to protect sensitive information. There are limits to it and ...what she said, I think we also have to be very practical and set expectations with the users as to what their obligations are.

Deven McGraw, Director, Center for Democracy & Technology

Thank you very much, Adam.

Adam Clark, Director for Health Policy, Lance Armstrong Foundation

Thank you. My question, it's a little bit more general dealing probably more with ethics than anything else. But relates around the minority to the majority status. And I'm more just wondering if you have any recommendations for the committee to consider as we look at the transfer, the obligation of the stewardship of that data for individuals where it was collected when they were under 18 versus after they've turned 18. As we look at cancer survivors, 65% of kids are on some type of clinical trial protocol. There may be later facts ten years later. Subsequently just we know even some cancer survivors don't ever want to be contacted again about their cancer experience or where those records might be. And when they are and they find out who has this, how did they get it, did their parents actually commit to this, so more of a general question, but if you've given any thought to that particular population.

Speaker

I'll answer it in a different way. I think the big issue is going to be in reverse where once genetic testing become much more sophisticated and advanced, and the parent has been tested for a certain genetic predispositions, and the child wants to go back and understand what maybe their parents were genetically predisposed to or there are issues associated with cancer and whether they should be tested for other things. I think that genetics in general is going to be a huge issue. And how do we appropriately manage genetic information with primary and secondary use is going to be huge. I think that's what I hear when I hear children and information flow.

Deven McGraw, Director, Center for Democracy & Technology

Neil, you're next on my list.

Neil Calman - President & Cofounder - Institute for Family Health

Two comments and then a question. So one comment is I agree with what you said about audit trails and stuff like that. I've had an opportunity to look at the audit trail on my own electronic health record. And every single time somebody runs a quality report or looks for adverse outcomes or look for everybody on

a particular medication, your name shows up and it gets to the point where it really relatively meaningless.

The second thing is in relationship to the example you gave, Eileen, about the abortion and somebody showing up in the emergency room, I haven't heard anybody really talk yet about the temporal relationship between when an event happens and when it's accessed. So, for example, if somebody had an abortion yesterday and they show up in the emergency room with a fever, that's incredibly relevant information. If they had it a month ago or a year ago, it might be completely irrelevant information. And so the timing between these events, if somebody was hospitalized for depression 12 years ago and that shows up on their record, that may or may not be relevant, probably isn't or if they were on a medication a long time ago. So I think we have to figure something around how this data is relevant in the records. I think that's some element we haven't really talked about.

The last part I wanted to make and just ask a question about really involves the public health piece, because I think public health isn't really about infectious diseases anymore. If anybody needed to be convinced about that when we started to talk about putting bio-terrorism and stuff like that in the hands of public health people, it became much more. And then I think the morphing of public health to really take into consideration chronic disease is really something that's happening more and more around the country now because of the burden of chronic disease on the population.

So where you mention the dichotomy between people being able to be on the subway and be exposed to something or not versus the elements of chronic disease, I think chronic disease is one of the most important things that public health has to monitor right now number one, because of the cost implications and number because we're being overwhelmed by it. And part of the policy piece of public health is that it has to inform the country about the kinds of focus that we need to have.

So, for example, Dr. Peel mentioned are former health commissioner in New York. One of the things they did was they started to collect information on diabetes. It's incredibly relevant to now know that for people who are in medical care in New York, there are over 100,000 whose last hemoglobin A1C is over nine, which means their diabetes is wildly out of control. I don't think anybody would have imagined that there were that many people who in medical care whose diabetes was that much out of control. And that allows for targeting resources and targeting interventions and other things that have to be done in a public health level.

So I'm wondering if you would comment on that piece of it. I don't really see that much of a distinction between the work we need to do around infectious disease and around chronic disease.

Speaker

Well, I would absolutely agree with you on a couple of things. The first point is on the time limited use of data. That actually is in my written remarks as well. I think that's a very relevant point and a system should accommodate that was well. I guess I would say I would go back to my point on public health and the data that's being collected is usually, even as Ms. Peel said, done under a statutory framework that has usually been actively debated in public forums as well as in legislative bodies. Those bodies are balancing different points of view. While there may on the relative level of importance, we absolutely agree with you that chronic disease is critical to the well being and to the health care costs of our citizen, however I do believe that if you look at where citizens are right now, they do have a fundamental difference on what they're willing to provide for information around infectious disease versus chronic disease. I think that some of the types of questions that we need to think about in that case is do we need individually identified data for that? Can we use anonymized patient level data? Can we use more population level data? How do we need to collect it?

So I think that there might be other ways to collect that data the protect people's privacy by either making it anonymized or collecting it at an aggregate level that actually can be very helpful in informing the policy debate. And I would think that that is another piece that is perhaps more unique to public health and secondary uses than it would be some of the discussion that we've had directly around treatment. In treatment, quite clearly you need individual identified data for treating the patient. In public health I think

you have to look at the function, what you're trying to accomplish and then decide what's the right level. It's almost like the minimum necessary to actually accomplish that public health purpose. That's what many of the debates often focus on is what is that right level and what happens, what are the limits of not getting every last patient's name, data, address and the ability to contact them versus anonymized or aggregated data.

Speaker

So just in relationship to the issue of being able to take people who in medical care and to be able to re-inform them that their diabetes is out of control and that these are people who are currently in care seems to me to be a public health issue. So I don't think it's only anonymized data that's useful in a public health context. You also need to in some cases be able to go back to patients and be able to understand the kinds of care that they're getting and to have a second mechanism of informing them that there are other types of care that they might need.

Again, we're doing that now with flu surveillance. There's only so much that we know about it at this point. At some point as you're collecting specimens, you might need to or want to be able to go back to people and reidentify people to inform them that there areof something that they might need to know about. So I'm just saying, it's not as clear cut as that, but I do appreciate the fact that a lot of this stuff that public health can do can be done with anonymized data.

Deven McGraw, Director, Center for Democracy & Technology

Thanks, I have three folks on the list here, Jim, Roger and Judy. So let's get through that and if there's time for those who aren't on the queue, we'll go there. And otherwise we'll wrap up, so go ahead, Jim.

Jim Borland, Special Advisor for Health IT, Office of the Commissioner, SSA

In the interest in keeping Deven's panel on time, I'll direct my question to John. You mentioned in the early part of your remarks, macro-level oversight of privacy and security for the NHIN. As a member of the NHIN coordinating committee, obviously I have a special interest in that. I'm curious, you went on then to talk about credentialing authentication agreements, allowing patient access to audit trail data, as well as their ability to limit their data and the ability to investigate an inappropriate disclosures. And while those are all obvious governance issues, I'm curious as to whether you believe that those kinds of governance practices are best made at the lowest possible level. Certainly you representing a provider organization and if you would agree with that, then what would you see the role and the scope of a macro-level oversight body?

Dr. James Golden – Minnesota Department of Health

That's a good question. Nobody knows how widely information is going to be shared. I just think there needs to be some type of oversight outside of the provider context when we're passing data between providers. If 99% of the data passes within a region and there is a local organization that that's responsible for that exchange, then maybe you can put that responsibility at that level. However, I think there needs to be national standards and there needs to be ways that that data could be aggregated in the event that there is transmission that goes on beyond a region.

I think at the same time, provider credentialing I think it incredibly important because not all providers are covered under HIPAA. Even with ARRA, we still have providers that are not billing electronically for services, are not covered by HIPAA. There's all sorts of boutique services that in theory could need to be part of the NHIN that aren't HIPAA covered entities. So therefore there has to be a way to insure that they act appropriately. And they're not business associates either, so it's a delima. There has to be those national standards established.

And I also think that we do have enforcement mechanisms today, such as the Office of Civil Rights. I don't know if you extend the Office of Civil Rights to have the role even at a regional basis for

investigating when a patient, I don't know why hospital X needed to see my information, I've never been there. But somehow you have to get that investigation enforcement out of the hands of the providers. I guess I don't know what level it resides at. But I think there needs to be national standards and the opportunity to insure that it's consistent across the U.S.

Jim Borland, Special Advisor for Health IT, Office of the Commissioner, SSA

Quickly, I would say that in thinking about exchange, what I think is different than a single provider is you now have three entities involved. You have a requester. You have a discloser and you have an exchange entity. All three of them need to be appropriate in their activities and their actions. One of the things that I think would be very helpful, if you think about investigating an inappropriate use or disclosure within that context, there might be information needs that you need to make sure that the requester always captures when they're requesting, the disclosure always captures when disclosing, and that the exchange is capturing along the way. So just capturing the information that would be necessary to do the investigation of inappropriate activity across those three entities and some mechanism for trying to use that information for the investigation would actually be quite helpful.

Deven McGraw, Director, Center for Democracy & Technology

Thank, Roger and then Judy, and if you both can—it's awful to be at the end of a list and closing out on time, but be as succinct as you can.

Roger Baker – CIO - Department of Veterans Affairs

I'm going to pass.

Deven McGraw, Director, Center for Democracy & Technology

Oh, thank you. Well, now we're early. Michael.

Michael Weiner – CMO - Defense Health Information Management System

I appreciate Neil's comment about chronic disease and the burden of chronic disease and the importance of managing population health. The other great example needing individual specific data in a population health approach is disaster response. What we saw in Katrina was that all those people in those shelters in Houston has chronic diseases and needed medications and didn't know what they were. So that's, I think, another great example.

Deven McGraw, Director, Center for Democracy & Technology

Many thanks to our panel. As we said at the very beginning, that we weren't attempting to use this hearing to answer all of the many questions, but to try to raise as many questions as we could, so that we could at the end of the day make some decisions about priorities and how to move forward and what might need some further inquiry. And I feel like you've definitely done that for us today, so I want to thank you very much.

David Blumenthal-HHS/Office of the National Coordinator for Health Information Technology

Thank you very much. This a lot easier having other people moderate. So I get to be the timekeeper. It's noon. We have a half hour break for lunch. I'll see you back here at 12:30.

(Break)

David Blumenthal-HHS/Office of the National Coordinator for Health Information Technology

I want to thank our panelists for being so prompt, more prompt, I'm afraid, than the chairman. We have more, I think, very illuminating testimony to be heard. Once again, I'm pleased to be able to ask, or maybe I can't ask, I'm not sure it's fair to ask you to do two. But I'm going Paul again to moderate. He enjoyed it so much that he wanted to do it again, he begged to do it again. Thanks to the panelists for being here and I'll let Paul take it away.

Paul Tang - Palo Alto Medical Foundation

Thank you very much, Dr. Blumenthal and good afternoon. I'm a last minute moderator. It's Dixie who is supposed to moderate apparently is under the weather, so wasn't able to make it. So that is why I'm moderating this panel. And the panel is called Models for Data Storage and Exchange, Aggregate Data, De-identification and Re-identification. It's a fascinating panel and the whole subject is absolutely fascinating subject. And as was described before, there are no PowerPoints slides. And also what we are really trying to do as a group is really information gathering. It's not like this is a deliberative process today. We're simply trying to learn information.

So I'm going to introduce each of the panelists. The first is Claudia Williams who is the Director of Health Policy and Public Affairs at the Markle Foundation. Claudia.

Claudia Williams – Director – Markle Foundation.

Thank you very much for the opportunity to speak and for giving us the longest name of our panel, which took two of three lines of my remarks here.

So our panel today addresses critical questions of privacy and public trust and in particular, the architecture choices to support trusted information sharing, which we've heard a lot about already today. My remarks will focus on three key points. First, as we think about these questions we must adopt a framework based approach; second, insure that policy guides technology and not vice versa; and last, that we can stimulate innovative models for protecting and sharing information because we need to do both.

As we've heard about already today, the potential of network information to achieve measurable health improvement is enormous. Access to and use of critical information whether recent lab values, discharge summaries, medication fill histories is literally the life blood of health improvement that we so urgently need. But this critical information is often not available when and where it's needed. Innovations that can improve care are disseminated painfully slowly; 17 years is the estimate from all studies. There is inconsistent delivery of proven care. As we know adults get 55% of what's recommended.

To address these issues, we'll need a 21st century health improvement, health information ecosystem. This will mean trusted distributed and dynamic access to information by authorized users, information management and architecture models that protect information while limited complexity and cost and feedback loops in quality research in public health to support rapid learning. The American Recovery and Reinvestment Act is a critical opportunity to unleash this potential. But the success of ARRA will depend in no small part on whether the public and health industry participants trust that information will be protected.

In 2005 Markle connecting for health articulated a policy framework for enabling information sharing while protecting privacy. This framework hinges on nine core privacy principles. The fair information practice principles that I think you've already heard about through several of the presentations today. The principles require that limits be set on data collection, that patients have access to unreasonable control over their health information, and that security safeguards are adopted.

Over the years, we have seen this framework translated into very specific practices within the health sector. Just today Mark Overhage talked about using this framework in his work. I think Phil in his comments will mentioned this overall framework as well. As we've seen this policy driven approach, we see several things. It means that when data are needed, the purpose must be specified. And only the data necessary for achieving that objective are shared. And that's really the core of the HIPAA minimum necessary requirements. Data usage sharing are made transparent through immutable audit logs as we heard about today and data stays as close as possible to where they are captured and are shared according to specific needs and with specific purpose.

In contrast a technology driven approach often starts with the technical requirements and is driven by technology decisions and then often comes to these critical policy matters in an after the fact kind of way. So what does this have to do with architecture? What does this have to do with technology?

I'd like to walk through a few examples of how these privacy principles can be the starting place for translating principles into operational decisions about how information is shared across the health care system. These principles should guide and shape the clear policies and technology choices, including how information is discovered, exchanged, analyzed and stored. The examples, though, are not meant to serve as readymade uniform solutions, but rather as illustrations. How can we use technology architecture to reach our goals? And remember our goals are these policy principles.

So let's start by looking at health information exchange. When we think about the principles of purpose specification, transparency, collection limitation and even data integrity and quality, the result is an architecture in which data are locally controlled. And we've heard some discussion today about this idea keeping data closer to the edges where patients and their providers are working together. And that doesn't just have important privacy protective attributes. It also has critical data quality and integrity attributes.

When the data remained distributed, that is, though, not necessarily comingled into one single database, but they can still be discoverable using directories and other technical tools that prevent the need to disclose all of the underlying data. Mark describes one version, the federated model, and in my comments, there's another description of one in Tennessee. But in both examples, you have these attributes of local control using architecture to protect information and keeping those data stewardship and data quality issues as close to the source as possible.

Looking at research, emerging approaches for research and analysis, benefits and the computational power of many distributed information sources, but not without necessarily the costs, time lags, privacy risks and data quality issues that develop when creating new aggregated databases that must collect, clean and centralize data before they can be used. The HMO research network is one example of a distributed health data network, allowing researchers to ask the same questions across multiple similarly structured databases housed in different organizations. This is the concept that we talked about at Markle about bringing the question to the data. So imagine that you have a research question. You have several organizations that have critical data on it. They're able to take that question to their own database and return results to you, but without returning all the source data, without returning all the identifiable health information.

Similarly on the quality front, today many quality efforts require participants to share personally identifiable health information to analyze and aggregate, look at quality as it exists across providers. But by contrast, New York City's primary care information project took a different approach. Physician's EHRs directly generate quality measures. Those are reported to Bridges to Excellence, which is a quality improvement P for P program. And there's built in mechanisms to audit, so you can go back and look at this data. You can go back and say on a such and such a day when you sent it to me, what information were you drawing on? You can still do audit of those results, but you don't need to send identifiable health information and you can still get to your important goal of quality improvement.

In public health the distributed initiative takes a similar approach to flu surveillance. Hospitals and clinics reports simple aggregate measures, not underlying identifiable health information. But let's step back. As we think about these critical population health examples, it is clear that there's not a one size fits all technical approach. We won't always be able to use the model that distribute uses or the HMO research network uses when we look at these questions. Every effort needs to start by defining why information is being shared and with what clear purpose. Guided by these answers, they can determine what information should be shared, what's the minimum necessary and what the technical approach should be. Often when we've heard examples from these folks who have really innovated these models, they think we thought we needed this much information, but when we really sat down and thought hard about it, this much would do. So this kind of rigorous analytic process can be hugely instructive to ask what do we really need to share to get to this goal.

It doesn't say you have to shut down the goal. It simply says that you need to ask how to do it in the best way. So in conclusion as we think about these critical policy questions that lay before us as we move into

this next century of what we hope will be networked information use, what are some of the key points to think about?

One, we should adopt a framework based approach, requiring that information sharing efforts funded by public dollar address three basic components of trusted information sharing: core privacy principles, sound network design, and strong governance and accountability. Those three must work together to create trusted information sharing. And two, let's insure that policy guides technology by using the basic tenets of fair information ... principles, such as purpose specification and collection minimization in the actual underlying design of quality comparative effectiveness, information exchange and public health efforts. Let's ask those rigorous questions. And third, let's stimulate innovative models for protecting and sharing information. How could we use these distributed research networks? What kinds of questions can we answer with that? How could distribute help us see a different way of public health reporting more generally?

Let's invest in the methodologies and strategies to address the analytic challenges of distributed analysis and develop approaches to share and use information that reduce unnecessary exposure through privacy protective architecture. Thank you. I look forward to discussion.

Paul Tang - Palo Alto Medical Foundation

Thank you very much, Claudia. Our next speaker is Dr. Philip Marshall who is the Vice President for Product Strategy of WebMD.

Dr. Philip Marshall – Vice President for Product Strategy – WebMD.

Thank you very much. It's a pleasure to be with you today. I'll be presenting just a subset of the written testimony today, a short introduction for you about WebMD to really color some of my perspective. WebMD began a number of years ago with really the consumer at the center of their set of services, whether that be for the public portal, WebMD.com, which serves over 60 million unique users each month or the ... WebMD health services division, which provides health and benefit management solutions to large employers and health plans that still with the consumer user at the center of that equation. So my testimony here today really by and large represents that latter division, WebMD health services, which delivers really data driven services built upon a user's own personally controlled, personal health record to large employers and health plans.

On the topic of the panel here today, secure data storage and exchange with the WebMD personal health record, the PHR services that WebMD are provided in conjunction, as I said, with our payer and employer customers, we have HIPAA business associate agreements in place with each of these that integrate professional data sources, like lab test results and claims originated data into the PHR, as well as data use agreements with the data partners that provide that data, be that TPAs, data warehouses or reference labs. The purpose behind data exchange with the PHRs is to allow our consumer end users to gather, store, manage and share their health data for themselves and to be able to share with others to help support better overall health care decisions. We do as you might imagine believe that the PHR can help achieve the objectives shared by multiple stakeholders in the health care system to provide a greater continuity of care in order to improve quality and lower costs.

Serving as a BA to covered entities, we do support and adhere to the HIPAA privacy and security rules. We do believe in giving our consumer users control over how their data is managed and shared. We do not share identifiable health information with employers. Although our end users can choose to share their data back with the health plans or the service providers that provide services on behalf of either the employer or the health plan, such as disease management services. Our guiding philosophy of consumer control and choice is as Claudia mention in line with the Markle Foundation's common framework and the consumer principles.

A couple of additional points and I'll finish up, I wanted to provide just a couple of points of feedback on some of the recent publications and discussions out of the committee. Those can be found, again, in my written testimony. The 2011 meaningful use objectives and measures specify getting access to consumers for their information. We certainly applaud the committee for the matrix of the meaningful use

objectives and measures overall. We did want to point out one discrepancy that existed in ARRA. There is the provision that consumers gain a copy and yet the 2011 criteria still describe access and so we wanted to point that out, so that care providers certainly can rest assured that when complying with the meaningful use criteria, they are also complying with ARRA.

We believe that there are certainly some specific barriers to consumer centric data exchange and access. We wanted to take this opportunity to point out one of them that we hear about quite a bit from our end users. That is some of the barriers that exist for them to gain access to their laboratory test results. This is, I'm certain, not a foreign topic to you all. But just to reiterate the point that consumers cannot get their lab results directly from the reference lab, but almost in all states, it has to be released by the ordering care provider. While it certainly makes sense as we look at what our health plan partners are able to do as a result of their contracts with care providers and what many larger systems are doing, such as Kaiser Permanente in releasing lab results to end users, we feel it's time to take another look at the legal barriers to consumers gaining access to their own lab test results.

Now I'll move on beyond that topic. That may be just a little bit of a side topic here.

So one of the other issues that we've worked very hard on that relates to the topic here at hand on data exchange is not just technical interoperability, which I think most of the standards work has centered around, but rather semantic interoperability. I think we somewhat uniquely being at the intersection of administrative data, lab test results, the consumer, employers, payers, we see data from a variety of different sources. So in order to create a consumer controlled and actionable profile for them to drive decision support services, we have had to manage how that data comes in and is then interpreted, so that it is actionable for the end user. As we look ahead to the standards that are being proposed, be it SNOMED, CT, RX, NORM, LOINC, we feel that semantic interoperability is going to need continued attention to insure that we are paving the way for the good semantic interoperability in addition to technical interoperability.

Finally when it comes to personal health record systems and certification, we do sit as member of the CCHIT personal health record working group. And as personal health records do play a role through interoperability in supporting the employees' criteria for doctors' offices and EMR systems, certainly we feel there is a role for certification of personal health records. So be that through CCHIT or through additional organizations, we certainly support that notion.

So with that, I'll turn it back over to you.

Paul Tang - Palo Alto Medical Foundation

Thank you very much, Dr. Marshall. Third speaker is Kenneth Beutow, who is the Associate Director of the National Cancer Institute.

Kenneth Beutow – Associate Director –National Cancer Institute

Thank you very much. I'm going to give just a quick second of background on the National Cancer Institute for those who may not be familiar with who we are and what we do. We conduct research is our primary mission within the National Institute of Health. But more importantly, we sit at the interface of care and an interface that we unequivocally believe is going to be transformed in the 21 century as we move to e-health universe in a learning health care system. Of particular relevance I think to this panel, though, is we have a broad depth of experience in conducting and managing information in support of clinical trials research, both national and international in scope. We conduct public health research maintaining large time monitored cohorts that are studied both geographically and locally. We maintain registries of aggregated and deidentified information that have both public accessibility, as well as regulated accessibility.

This long history of large scale data acquisition management use and disclosure includes managing health information exchange between and entities, virtual communities. We've had actually put in place both policies and technical infrastructure that supports that. We've explored more models than you probably could enumerate on how to monitor, authorize, control and exchange information, some of which

are very similar to you, I'm sure, members of these groups in institutional review boards, data safety monitoring boards and a variety of other local types of access communities. What I wanted to do was just spend a minute or two sharing over and above what's in the testimony, some of the lessons learned.

I want to be explicit that I don't speak for the National Cancer Institute or the National Institute of Health of the Department of Health and Human Services or for any entity of the federal government. I'm going to be giving my personal comments and reflections on what we've experienced through a large scale nationwide national at work, the cancer biomedical informatics grid and how it's touched all of these things above.

So first and foremost in my testimony we described the information flows where we have use of identified, deidentified and aggregated information. That gives to point one that I want to me. And that's one size just simply doesn't fit all and we have to be absolutely cognizant as we move forward of trying to find single sized solutions. We need information architectures that recognize that data has to live in all of these different forms and more importantly, has to have the capacity to be transformed between these different pieces.

Number two, definitions are important. Structure is key. Research collects data in highly structured ways. One of the ways that we can do these transactions that I just mentioned is because of the discipline as part of the research process that sees to it that we collect data in structured, common data elements in information models that lets us know and potentially where necessary, control the providence of data, who has access to it and under what circumstances. If we're going to do segmented data access, we can't do it in the absence of information structure. There has to be architectural frameworks around this.

I want to be actually crisp on this. When I say architectural framework, I know it actually gets the hair on some people's neck up. We're not saying that there is specific prescribed technical solution to a problem. What we're saying it that there needs to be, again, a semantically interoperable framework that allows us to describe what information is, where it resides and have data about data. And it needs to be transparently accessible and only through that transparent accessibility of data about data can we help to manage to who has access to what. So we think this is critically important. We believe there needs to be—this then facilitates the creation of distributed trust fabric and an architectural framework that allows us to manage both at a local level and at an aggregated level information.

Next point, we believe it's critical that we manage appropriately the grain size of consent. We actually recognize the importance of consent where is practical. But we also recognize that there is as has been discussed, key public health uses and the expanding definition of public health that needs to be constantly considered in all of these. We need to also be constantly aware of the burden of consent as well. And that burden can fall in several different ways. How aggressively do we want to be pressing sick individuals or people who are currently diseased to be providing consent or can we deal with this in other ways? We run into the issues in my field unfortunately of deceased individuals and how we go about managing the consent associated with that.

I think, though, one of the exciting things about emerging architecture and technology is it empowers us again to not have a one size fits all for consent and to be able to tag consent in either blanket fashions or in individual grain size fashions, depending on the specific use. Our solution to dealing with this is architectural frameworks, and I will apologize for my technical dive here, is to use attribute based access layered on context sensitive role based security. So that's a mouthful. But that being said, the mouthful that that is actually an infinitely doable thing that we have deployed in our nationwide network through the cancer biomedical informatics grid where at the level of individual attributes, we can actually track who can do what to what and in what context.

Lastly in the context of specific points, we believe it's important that we don't create a regulatory framework that tries to prohibit all possible misuses, but instead achieve a balance that punished misuse. We think it's dangerous to assume that we can ever regulate a framework where data won't be misused. And if we tie into the knots, we actually do have the potential of doing more harm than good. We believe we need to audit and enforce.

Lastly, I have one emphatic plea. Please do no harm. Why do I say that? Research lives in a very highly regulated universe today. There are many, many restrictions. Many of the issues that you are discussing we live with on a day to day basis in terms of who can access what in what circumstances with what technologies with that what approvals and with what institutional and individual consents. Please be careful as we move forward with the electronification of health information that we don't layer on an additional layer of bureaucracy that breaks a systems that's already somewhat on its knees at time to conduct research. We need to be very careful that as new rules are passed, new regulations are put in place, that we don't have viral unintended reach-through that actually cripples existing working processes and that were explicit in the boundaries of where rulemaking sits. And explicit in the boundaries of existing regulatory frameworks, so that we don't compromise our capacity to do things that we can already do.

We have a long history of indicating that research and care can coexist. I point out, and Adam pointed out that power of pediatric research where 65% of individuals are both engaged in clinical care and in clinical research. We believe in the cancer community that that's one of the reasons that we have had a 50% improvement in cancer outcomes in pediatric research as opposed to some of our other areas where we have less than 5% participation in clinical research. We also believe that it's one of the reasons that we've seen things like acute lymphoblastic lymphoma move from a death sentence of about 5% survival about 40 years ago to about on average 87% survival and for some sub-forms, molecularly type sub-forms, 95%.

Research is this engine of information that we heard referred to earlier that will take us out of being so 2009. And unless we actually have the capacity to drive that, we won't be able to move forward. Moreover, if we want to achieve a learning health care system, we have to intimately join these two universes. So thank you.

Paul Tang - Palo Alto Medical Foundation

Thank you very much. Policy committee, do people have questions. Let's start with you, Tony, and we'll move to Paul next.

Tony Trenkle - Director of OESS – CMS

Thank you, Paul. Thank you, speakers. I have a question that just relates to the aggregation of data. As you know as we move forward with meaningful use and collection of data under high tech, it presents some interesting possibilities as we continue to refine that over the years. I wanted to get, I think, Claudia and Ken in particular to address this at some level. But I'd like to see if you have any specific thoughts or guidance as we move forward in this area.

Claudia Williams – Director – Markle Foundation

I think an issue that your agency is already very interested in and engaged with is a question of how quality reporting could be done in a more direct...way as a result of using health IT systems in EHRs. I think that idea that the demonstration of achievement of meaningful use could be accomplished in a way that's embedded in a regular use of a systems perhaps A) lessens the burden on the providers and B) provides some additional opportunities for the kind of data protection mechanisms, reporting aggregates, saving states that you can go back and audit that have been more difficult to achieve than more traditional quality reporting approaches.

So I don't have the technical answers. I know you have questions you're trying to answer about how to accomplish that. But just to say I think it's an incredibly an important area of exploration and resolution as we look forward.

Paul Egerman – CEO – eScription

I would will argue even in the definitions of when we're talking about certified electronic health records and we talk about the need to have clinical decision support and other activities, the availability and use of aggregated data is going to essentially be essential. But the engine that drives much of this underlying decision support is the access to and projection on to aggregated data. I do think, though, that I have

some sense of responsibility to suggest, though, that we need to be even careful that when we use the word aggregated, it doesn't necessarily mean that information is completely deidentified and that there is no risk whatsoever of flavors of extracting individual information from that.

I think one of the ways we deal with it or try to deal with this in a clinical research setting is to be as up front, transparent and honest with people that contribute information into these resources, to never assure that there's never a chance that any information could be disclosed about them. So it's a flavor of informed consent, but I think we need to be constantly exploring these and figuring out how we get next generation tools that support this.

Paul Tang - Palo Alto Medical Foundation

Thank you, Charles.

Charles Kennedy - VP for Health IT – WellPoint

It's hard to get your questions, so I'm going to try to get in two for one. First question in full disclosure, we've been working with Phil's company for five years. I checked with our security and privacy office and we have about 25 million members or so with access to PHRs through your system. We haven't had one privacy or security complaint. I was wondering if you could comment on from your perspective why you've been so successful in supporting us from a privacy and security perspective.

And then to squeeze in the second one, for Ken from a personal...looking at oncology and personalize medicine, maybe looking five years down the line, if you could comment on what types of things we should be thinking about from a privacy and security perspective with that expecting to impact oncology.

Charles Kennedy, VP for Health IT, WellPoint

So in response to the first question, when you consider the fact that I believe we began professional data feeds into the personal health record on behalf of the WellPoint membership, somewhere in the order of 2004, early 2005, even though all of us who are in this room I'm sure have been working on these issues and ready for this transformation in health care for a number years, perhaps more than a decade, the truth is that most consumers out there, be it members of a health plan or employees of an employer are just being introduced to this. So the idea of you have data on me and you're giving me control over that data to use as I see fit, whether it's driving services or it's sharing with care providers, I think is something that can be enlightening. It is new, but it's also something that I think patients accept pretty readily. Like you, we've been please with so far is the fact that they do see value in it. They don't see it as a threat to their own privacy, but rather as an enabler of their privacy. So that's what I'd say.

I would also say that we continue to work with consumers directly to really understand what their sensitivities are and try to be mindful of it. As we continue to increase the percentage of participants within all the organizations that we serve, we're trying to be mindful of that. But I think it's such a new realm and so far, people seem to be happy with the idea of it.

Kenneth Beutow – Associate Director –National Cancer Institute

And just quickly, I think there are clearly moves, the transformation that's about to be happening in cancer related to having detailed molecular characterizations that are going to be driving treatments I think are going to be critically important in medicine. But I'm not sure radically in the context of fingerprints that can deal with issues associated with privacy and security are fundamentally different than some of the other issues that you're going to be dealing with. So in other words, I think you all have heard testimony from others and almost everyone is familiar with the ability to reidentify people from actually relatively small numbers of people, pieces of key clinical information. While it may be a single piece of information in a genomic profile that would be sufficient for that, and we'll have to be careful as to how we facilitate people's access to this.

This is one of the places where I come back to that we need to punish not prohibit. And we need to regulate what are acceptable uses of this information. And when people violate the acceptable uses of this information, just the same as somebody steals my credit card, I punish them, we punish them for

misusing that information in all sorts of ways. I would actually argue if somebody steals and misuses my genetic profile and/or my information profile, we should have the capacity to punish them.

Charles Kennedy, VP for Health IT, WellPoint

This question is, I think, for Phil in the area of PHRs. You heard from Jody that one of the things that both the ONC is preparing may get some of the input from this committee is on the PHRs from non-covered entities, which you're representative of. So I heard you say that the purpose for your PHR is to serve the individual. You also said that you are HIPAA compliant, I think were your words. So would there be any objection to a recommendation that PHRs by non-covered entities follow the same, basically have the same relevant provisions of HIPAA? You certainly wouldn't have all the—you don't treat or anything, but would all of the other kinds of provisions of HIPAA then be acceptable to a PHR from a non-covered entity, do you think?

Dr. Philip Marshall – Vice President for Product Strategy – WebMD.

Since we serve as a business associate of covered entities today on behalf of—I'm going to venture to guess 50 organizations or so, then I believe that we say yes because we signed that document that says that we are. Now I know that there are differing points of view as you all have heard differing points of view from those who represent PHR systems that are consumer controlled. But that certainly we feel very comfortable within the requirements of the HIPAA privacy and security rules.

Charles Kennedy, VP for Health IT, WellPoint

Then when you have these contracts, what are the people who contract with you expecting in return from you, whether it's a health plan or an employer? What are they getting in return from you?

Dr. Philip Marshall – Vice President for Product Strategy – WebMD.

Sure. As a service provider to their beneficiary, they feel that a more engaged consumer who has greater transparency around their health information and has services that are driven from that actionable data choosing their benefit plan, looking at the hospitals in their area and which one might be best to serve their needs, looking at their treatment options or medication costs or alternatives, really centering all of that around their own profile, the wish the end user could be more engaged and active consumer with their health care. They see that as having really a variety of different benefits as you might imagine.

Charles Kennedy, VP for Health IT, WellPoint

So there's no data aggregate or otherwise given back to any of your sponsors?

Dr. Philip Marshall – Vice President for Product Strategy – WebMD.

As actually is in the written testimony, we do have aggregate data reporting that they have access to. This is deidentified reporting with additional cell sized drill-down protections to prevent any ability to infer identity. So those are mostly in the areas of usage of the services and in a person's health risk assessment profile, but again, at the aggregate level looking population wide. To the extent that the consumer chooses to share data with additional service providers, such as disease management services, they can do so. And that is a common part of the array of services that might be delivered.

Charles Kennedy, VP for Health IT, WellPoint

If I could make one comment on responding to Ken's couple statements that aggregated data is not necessarily be identified and can be reidentified. So how would you get over that when you're sharing back to. We do know that employers and health plans are two of the entities that consumers have some concern over. So with respect to what Ken said "aggregate data," how would you respond to that one?

Dr. Philip Marshall – Vice President for Product Strategy – WebMD

In fact, I feel after having watched this play out for the last ten years, that we have helped these organizations actually provide a service where they're using the trust that we have with the end user to help them feel assured that they're not using that data inappropriately through us, at least. Of course, we have no control how a covered entity might use that data otherwise as they're legally authorized to do. But when it comes to our service in addition to deidentifying the data that goes into the data warehouse,

we also do limit on the reporting of things, drill down to a 50 minimum cell size, so that inference of identity is limited. So that's an additional measure that we take.

Paul Tang - Palo Alto Medical Foundation

David, did you want to say something?

David

I've had many questions, but I will limit myself to one just to try to role model. So I guess it's for Dr. Marshall and it has to do with the nature of the personal health record that you maintain and this question of individual access and the ability to modify, the patient's right to modify the data. So I assume you have claims data, but also some clinical information in your personal health record.

Dr. Philip Marshall – Vice President for Product Strategy – WebMD

That's correct. We take claims data and transform that into the person's health history to the extent possible for administrative data and then also lab test results be they through screening services or from the clinical laboratories.

David Blumenthal-HHS/Office of the National Coordinator for Health Information Technology

When patients get access to this, do they have the right to modify it?

Dr. Philip Marshall – Vice President for Product Strategy – WebMD

I believe that it's a line of questioning. That was a line of questioning, absolutely. So it is our belief that that a consumer should not be able to alter professionally sourced data, but to be able to addend that data, add notes to that information or augment that information as they might see fit. But in the end, they also do just control overall how that data might been or shared through our system

David Blumenthal-HHS/Office of the National Coordinator for Health Information Technology

So now that I understand, I can ask my question, which is can you imagine circumstances and how would you balance the patient's right to "control the data," and modify it with a professional's standards and needs? Ken spoke of the importance of structured data. If we're going to use distributed data sources to do clinical effectiveness research, post marketing surveillance, disease monitoring, all kinds of public uses, we need to know the data is comparable. Yet patients do have an undeniable right to access their data and increasingly, it's accepted that they have the right to modify it. So do you have a solution to that? Obviously, you don't allow them to do it at this point, but could you imagine a situation where you would?

Dr. Philip Marshall – Vice President for Product Strategy – WebMD

As you might imagine over the last ten years, this question has arisen a lot since the idea of a consumer controlled health record is a new concept to care providers as well. So the truth is that I have really yet to see much of a conflict arise in reality in that, the consumer in really gathering, storing, managing, sharing their data is the one who is most incented to make sure that their data is complete and accurate. And the truth is that most of the health records that sit within the providers' offices are provided verbally by the patient. And the personal health record helps be a more complete representation of their information. And really honestly, rarely do consumers choose to withhold information from their treating care providers at least in my experience. And so in that way, I really haven't seen much of a conflict.

I will add one caveat that when patients do withhold information for purposes of privacy and our product does allow them to designate in any data element as being private to them and sensitive, that we do within the provider view of information that they make available to care providers, we do have a notification that it does not represent all of the information that may have arisen.

David Blumenthal-HHS/Office of the National Coordinator for Health Information Technology

I guess just a couple thought from some of our work, one, that as we think about the PHR, keeping that conception that it's a copy of the data that's under the management and initiation and control that the PHR wouldn't accept for the initiation by the consumer and they get a copy of their data to manage it in the tool of their choosing. Secondly, I think we've seen some recent news reports where just showing

how evidently, data quality ain't great in the country and there's a lot of data out there that could benefit from transparency and, frankly, correction using a consumer's knowledge and information and experience. So what I think that what that invites us to do is think about the most operationally workable mechanism to let there be a dialog between the provider and the patient around the accuracy of their data, so that patients have an opportunity to help correct it and improve the quality. So I think that we need to see it as a positive some way of saying there's a huge amount of information we're not capturing right that could help improve data quality. And a lot of it comes from the consumer.

Kenneth Beutow – Associate Director –National Cancer Institute

Just a very quick comment on that, in the regulated framework, we have to deal with this type of issue, not atypically, especially when you're doing FDA submissions and other components. One of the ways that's dealt with is by auditing and providence logs, so you actually track the history of each data element and who made what changes. And then those could be reviewed by whatever appropriate authority and the credentials of that group can be evaluated as to how reliable and definitive it is. So by having that edit and audit log and who made what changes allows you to actually be able theoretically be able to explore some of those challenges.

Deven McGraw, Director, Center for Democracy & Technology

I have three questions

David Blumenthal-HHS/Office of the National Coordinator for Health Information Technology

Okay, Deven. We're running short on time.

Deven McGraw, Director, Center for Democracy & Technology

Yes, I know. I'm only doing one. I'm only doing one and it will be a real one this time. I'm not trying to put you on the hot seat, Phil, but we have directed a lot of questions your way and here comes another one. You mentioned something about supporting certification of PHRs and we recently in this committee adopted a set of recommendations that recommended that certification be very narrowly focused on the functionalities that are needed to meet meaningful use in an EHR context. Even with respect to sharing data, and again, since the meaningful use payments are going to physicians, who are going to have to demonstrate that they've got a system that meets that criteria and is certified to meet those criteria, it's a much narrower, I think, process than was historically the case with respect to what the certification commission considered and used as criteria. So I know that CCHIT is pursuing certification for PHRs, but now that we've kind of more narrowly construed what we want certification, at least from the Policy Committee standpoint, to be focused on I guess I'm sort of curious what the role of sort of certification in an official way would be if PHRs, which are not going to be bought with physician incentive payments and maybe it's more of a sort of Good Housekeeping seal of approval that it's meeting certain benchmarks, but I'd like for you to comment on that if you could.

Phil

Sure. First of all, as a member of the Personal Health Record Working Group at CCHIT I actually fully and completely agree with the limited scope of certification in ensuring that a personal health record does, with regard to its privacy policies, security practices and interoperability capabilities, are able to support the meaningful use criteria. So I fully agree with any certification actually focusing on that. That's certainly what I'm going to be, as one member of that workgroup, pushing for.

I can tell you that in our experience in responding to a whole multitude of requests for proposals from health information exchange, health record bank initiatives, health plans, who wish to have PHRs for their membership, employers; that there is a desire to make sure that somebody has put these systems through some rigorous testing as they adhere to certain principles and practices. So I think in that way they could also be helpful to a variety of stakeholders, but I agree to the point that that initial certification

in 2010, which will be, hopefully and likely, our first year of certification will be focused on supporting the meaningful use patient engagement criteria and the privacy and security provisions.

David Blumenthal-HHS/Office of the National Coordinator for Health Information Technology

David Lansky, I think you had a question.

David Lansky, President & CEO, Pacific Business Group on Health

I think both, Ken and Claudia, you talked about architecture and the ability to utilize architecture as a means of increasing privacy protections and other features. As a committee, we have not said a lot about architecture. As we get further into the HIE world the individual states, who are implementing HIE governance and implementation programs will have to think about that. I know certainly from the ... work and from CA grid there is a lot of experience in recommending elements of architecture that are privacy enhancing or protective. I'm wondering how you might give us your guidance or your opinions. Probably what I'm thinking about is back to Tony's question. Quality reporting is one set of applications. Comparative effectiveness research and the federating of existing registry systems for a variety of purposes, like the HMO Research Network has done, are sort of the next generation of use of the interoperable National Health Information network and it seems to me we need to think about having opinions about architecture fairly soon that help achieve the goals we're talking about today; that we would then some way propagate or recommend or even tie to meaningful use in some way. I haven't thought about that at all. Can you just give us your reflections on how, as a policy matter, we should think about architecture?

Unidentified Speaker

You know, when I was writing the comments I really kept on trying to skip the first part where we talked about the policy framework and skip right to the architecture and it just doesn't work. So I think one is to really, first, establish or ..., lay in front of you word of the policy goals that we're trying to accomplish and the privacy principles that we're trying to put in place that would be cross cutting across these efforts.

I think, second, there is so much ongoing work in this area. I know there are new efforts that have been trying to reach funding across large clinical delivery systems using a similar architecture. There is a lot we don't know within the research space about how to use those and what the limits are and what we can learn from them.

So I think, I guess, three things: One is this committee could be hugely helpful in saying here are the privacy principles and guidelines that we need you to think about when you establish architecture, so draw that direct, bright yellow line link between the privacy goals we have and the architecture choices you'll make and technology.

Second is to really cultivate and use these federal dollars to cultivate these other models that ultimately will allow us to have these incredible learning opportunities and not assume that there's only one architecture that has to be centralized to accomplish that, so there's a lot more we need to do in that domain.

Third, I think, is lots of HIE efforts today are using what we call a federated model using RLS. There is a lot of really great experience about how that works. There are a lot of questions that need to be answered at an individual. I know states are busy at work; California is trying to figure out what their models are going to be, so I think you could play a huge role. I know the NGAA is having a meeting this Friday to work with states to basically to say to states, "Here are five examples of where this is working and the architecture they picked. Here's what they have learned. Let's put you guys together and have you learn from each other. This is working today. It's not new stuff. There are really good models out there that

are already in effect that have years of experience now that could really be instructive in helping other states." The states that are just now setting up HIE probably also have less expertise. They didn't do it five years ago because they didn't have the expertise and initiative to do it and they could really use some help, frankly.

Phil

I am completely in agreement. I want to augment with two things. I unequivocally believe that policy needs to drive architecture, but what I think we need to have a crisp articulation of is that policy does include architecture that supports quality, CER and these additional, important learning health care system uses of the information, so the architecture has to account for these and has to then have the appropriate attributes necessary to support these, have the necessary attributes to support the flow of information into the resources that perform quality CER, other things, as well as the transactions necessary. So I think it will be essential to have that be specified.

David Blumenthal-HHS/Office of the National Coordinator for Health Information Technology

That's great, Phil. Thank you very much. We've completed the time that we had allocated to this panel. I just want to say thank you very much for a very much informative presentation.

Unidentified Speaker

Great. Thank you. Thank you, Paul. Thank you to the panel. The next panel is going to be on transparency, audit and accountability. Our Privacy Task Force cross cut across both the HIT Policy Committee and HIT standards and Steve Findlay is also a representative of the HIT Standards Committee and he'll moderate for us.

Steve Findlay, Senior Healthcare Policy Analyst, Consumers Union

This panel is our next to last one. I think we have one more panel and one person on that panel. There are two folks on this one. This panel deals with the subject of transparency, audit and accountability and includes Bob Gellman and Robin Omata. Which one of you wants to go first? I'll introduce you, Bob.

Bob Gellman, Consultant

Alright.

Steve Findlay, Senior Healthcare Policy Analyst, Consumers Union

Bob is an Independent Privacy and Information Policy Consultant. He has years of experience. Many in the room know Bob well in the privacy area, working for a variety of folks, but he's now a consultant and independent.

Bob Gellman, Consultant

Thank you. Thank you for the invitation. I have a statement, which covers the topics I was assigned and a few others. I have views on lots of issues in this space. I'd be happy to answer questions on any of them, but I will stick in my comments to what I was asked to talk about. I want to begin by talking about accounting.

For any fully computerized system of health information it's essential that there be accounting for all disclosures and all uses. Uses are internal to the facility. We've already had testimony here today from John Houston that that capability already exists and is utilized. The celebrity snooping cases illustrate that when these problems arise hospitals can go into their systems and find out who internal to the system, internal to the hospital looked at records. This needs to be done consistently. It needs to be done thoroughly. It's an important measure of accountability. It's an important protection to track down what happens with medical identity theft, which is a very serious problem and for which any kind of fully computerized health network system, whatever you guys are planning, is going to be an engine for the growth of medical identity theft. Without accounting there will be no accountability.

The second point: The patient should have on-line access to their accounting records. Now, I don't mean that as a totally abstract thing. If they have on-line access to their health records in some fashion the accounting records should be available. I should be able to go home from the hospital and look up and find out who saw my records when I was there.

I hesitate. I did not include in my statement the recommendation that there should be an affirmative disclosure of accounting; that I should get an e-mail when someone looks at my record, but Gayle, I believe, earlier this morning talked about that, so I see I was too conservative in my recommendations. I think that should be available to patients who want it. There are all kinds of ways of doing it so that I'm not admitted to the hospital and then come home and find I have 4,000 e-mails telling me all of the people that saw my record.

The third point: If accounting records exist then a patient should have a right of access to them. Right now under HIPAA there is a limit to how long accounting records have to be maintained. That was also affected by the legislation. If the records exist the patient should have a right to see them and that includes records, accounting records that are not required by HIPAA. If a hospital has internal accounting records, whether required or not by law, patients should have a right to see them.

A fourth point: I recognize that there are costs involved in doing some of these things. I think that any new requirements for accounting should be perspective only. They should only apply to computerized records, not to paper records. I don't think anyone should be asked to account for oral disclosures of records. It's simply too cumbersome and too expensive. I think that if HHS in rating HIPAA had said everyone has to do accounting, but no one has to retro fit an old computer system most of the problems would have gone away. If everyone is told that new computer systems have to have this capability all of the capability will be added and can be operated with very little expense.

One omission from HIPAA is that there is no requirement for accounting for consensual disclosures. If I authorize a disclosure as a patient there is no requirement for the hospital or whoever to account for that. I think that is a terrible omission. What is going to happen as records become computerized is patients will be asked for consent by people all over the place; Web sites, car dealers, anyone who can get access to my electronic health records can turn them over to junk mail America, who can then exploit them for their commercial value. I think this is exactly what will happen and patients will have no idea that the 27th paper they signed when they bought a house or they bought a car or they got a loan actually authorized somebody to get copies of their electronic health records. Unless there is a record kept of those disclosures the patient will have no way to find out that they did authorize it and no way to go back to the covered entity or whoever the record keeper is and say stop doing it. It's a very major omission.

The ARRA legislation included a provision, which I call pass the accounting buck. It said that a covered entity doesn't have to keep track of disclosures or provide an accounting of disclosures by business associates. Instead, the covered entity can just give a patient a list of business associates and the patient can then go pursue all of the business associates to find out what they did with their information. This is a disgusting provision. It's almost impossible for anyone to use it. There will be no accountability in the system. A patient could spend years going from one business associate to another just to find out if they even have records or whether they disclose them. It's completely impractical. Can you imagine? A major hospital could have hundreds, literally hundreds of business associates. If I have a list of those and I'm a diligent patient and start contacting them all, all of those hundreds of business associates are going to say, "Who are you? Authenticate yourself. Prove to me that you're really Bob Gellman, covered by these records before I'll even tell you whether I have any records." It's just completely impossible, the legislation. This is a provision that did not belong in legislation. There are some issues here, but it was handled very badly and I think that there are ways of dealing with this.

Finally, my last point on accounting is something that John Houston talked about. Covered entities should be required to use accounting records for oversight. He talked about how that was done. I'm not going to go on beyond that, but that's exactly what needs to be done. It should be a requirement.

Let me make a couple of comments about transparency before I finish. The current HIPAA rule on transparency, on what to do with notices of privacy practices asks healthcare providers to make a good faith effort to obtain from a patient a signed acknowledgement that the patient received a privacy notice. This is absolutely the worst of all possible worlds. It is a paperwork requirement that no one on either end of the transaction understands. It's completely meaningless. Patients sign these things all of the time. They are not offered privacy notices. They don't want privacy notices necessarily. It's just a meaningless paperwork requirement and it ought to be eliminated.

What should be done in this area? I don't think you can measure success by whether patients get a notice or whether they read them or even whether they understand them. I think it would be very nice if notices were understandable. If I have a recommendation it is don't let lawyers write notices. They write incomprehensible verbiage and no one can understand them. I think lawyers are sometimes rewarded for writing notices that no one can understand. I'm a lawyer. I've done privacy for 30 years. I get notices from banks particularly that I cannot understand even though I diligently read them and try and figure out what it is that they're telling me.

I think that what's important here is that patients have the information available to them when they want it. That means having written notices that they can ask for, having it on Web sites. Most patients don't care about their privacy rights most of the time and I don't think there's any reason to force it upon them. When the patient cares about it, when they have a concern, when they want to see their records, when they think their rights have been violated they will seek out a notice. They will read it and they will pursue their rights. That's enough for me. I don't think we need to impose additional cost, additional paperwork requirements that don't help.

That's it. I will be happy to answer questions.

David Blumenthal-HHS/Office of the National Coordinator for Health Information Technology

Thank you, Bob. That's terrific, just terrific. Robin Omata is a Lawyer and a Ph.D. She is a National Practice Leader in the Ethics and Integrity Office in Kaiser Permanente. At a previous job Robin served as a Chief Privacy Officer for United Health Group.

Robin Omata, Lawyer, Kaiser Permanente

Thank you very much and thank you for the opportunity to participate today in an important and difficult consideration of privacy and security in the coming world. I'm representing today the Kaiser Medical Care Program, which is the largest private integrated healthcare delivery system in the U.S. today. It includes the Kaiser Foundation Health Plan, the Kaiser Foundation Hospitals and the Permanente Medical Groups, which are independent physician practices that contract with the health plan to meet the health needs of our membership, which is about 8.7 million members in nine states and the District of Columbia. I'd like to make four main points today and actually fast forward to the disclosure accounting issues as time allows.

The first point is that healthcare dollars must be directed to value-added investments that provide measurable benefits to patients.

Secondly, the accountability and transparency of HIPAA covered entities are essentially already largely accomplished through existing privacy and security compliance requirements.

Thirdly, with respect to the American Recovery and Reinvestment Act of 2009 we respectively suggest that the disclosure accounting requirement as currently written does not add value relative to the cost of implementing the requirement as currently written.

Fourthly, we recommend that the meaningful use measure that uses a confirmed HIPAA privacy and security violation as a basis for measuring privacy and security protections of the EHR be revised or eliminated. I will elaborate on that later.

I would just like to list a few statistics on our organization to give you an overview of the scope and scale of our work that informs these comments: Kaiser Permanente operates and owns 35 hospitals and 431 medical office buildings in each of the nine states. Where we do not have hospitals we contract outside for that care and independently there are referral needs for other ambulatory and hospital based care. Last year we recorded over 36 million provider visits, over 500,000 surgeries and about 130 million prescriptions were filled, so that's quite a bit of throughput and per member it's significant encounters with the medical system. In the same year about 300 members used My Healthcare Manager, which is our on-line health record and it's a view into Health Connect, which is our trademark health record. This healthcare manager allows patients to securely access their healthcare records from home, as well as e-mail their physicians, refill prescriptions, make, change and cancel appointments for themselves or for family members and to view lab results at no extra charge. In each month about 600,000 secure e-mail messages are sent to Kaiser's doctors and clinicians and more than 1.6 million lab tests are viewed on-line with 1.4 million requests for appointments made via this accessible device.

This is really only intended to give you a sense that we are already connected; that we take very seriously not only the capabilities and functionality of the system, but the security and privacy that must obtain. We remain deeply committed to the improvements of our systems, which include Health Connect, but all of the ancillaries as well, so lab, pharmacy, prescription systems, which are not part of a single record, but which contribute to a unified view of a patient's record.

That's all to say that there's a lot being bandied about about the EHR as a single entity, as a single thing, but it's really many different systems combining and as others have talked about legacy, homegrown systems, it's a lot of things to manage and we're moving forward on that. Nevertheless, I think that our care is really the focal point on improving the utility of the EHR to support healthcare delivery that is measurable to the patient and to the community. On balance, the overriding consideration in adding features and adding requirements, whether they be clinical or regulatory, is that the ultimate benefit is to the core objective of delivering high quality care at an affordable cost.

I'd like to right now move to the disclosure accounting requirements, which we think, without further clarification, as written in the regulation, in the law represents a significant troubling and burdensome compliance requirement with excessive cost to uncovered entities without producing meaningful benefits to members, patients, clinicians or regulators. We respectfully request that the committee do the following in support of the promulgation of regulations as required:

Number one would first involve the definition of what constitutes a reportable disclosure.

Secondly, provide a definition of what it means to use, maintain and collect protected health information through an EHR.

Thirdly, to provide a definition of what constitutes an EHR for the purposes of disclosure accounting that is more detailed than the current definition contained in the legislation.

Fourthly, to exempt disclosures as defined under the HIPAA privacy rule between entities within an organized healthcare arrangement. That's a little inside baseball. We could talk a little bit more about that.

Finally, we would hope that the committee could consider conducting a survey of covered entities to understand the national experience and cost associated with the accounting of disclosures as practiced prior to the enactment of ... and to understand the effect that the new requirements will have on covered entities. This is not to argue against the requirement at all, but to have more information in order to make it meaningful and to balance the cost for the benefits.

Now, looking at Kaiser's experience, the impact of the current requirements could involve as low as 2% to 3% of our out of network admissions and visits in the regions, which have basically a very compact and comprehensive network itself. We have, in those cases, fewer visits going out of our system to as many as 100% of admissions for hospital based care in the region. All of this is simply to give you an idea of

the scale of the effort to account for activity that is related to treatment payment in healthcare operations that's not currently tracked in the manner that's required under the legislation.

In addition, depending on the interpretation and the rule making and implementation, routine data exchanges for TPO purposes between covered entities within a single organized healthcare arrangement could be considered disclosures and would then be required for accounting as well. We would consider that burdensome and not adding value either to the patient or to our current treatment obligations.

Based on our experience also during the calendar years from 2003 to 2008 and using the more narrow definition of disclosures prior to ... HITECH, we believe that the consumer/patient demand for accounting of disclosures is extremely small. We recorded fewer than 350 requests cumulatively for accountings and disclosures during that 6-year period. For each year that would amount to 1 out of 130,000 patients. So based on our experience, we believe that the number of individuals, who may request the accounting of disclosures going forward will be very, very small and disproportionate to the work effort implied by the requirement.

We believe that significant diversion of limited capital and human resources at this critical time and stage of EHR adoption and enhancement would be unfortunate and it's possible that this misdirection of resources could be enough to curtail adoption by some organizations due to the limitation of funds and staff resources to accomplish the work or rework to satisfy these obligations. At the very least it would represent a material increase in the overall cost of adoption. So that's to layer on additional capital cost of borrowing, etc. for smaller, but also larger organizations, who are moving more slowly towards adoption. For Kaiser, since we've already adopted, since we're enhancing our systems it would mean simply another cost that enters into the accounting and disclosure process, but it is a significant cost.

I'd like to talk a little bit about the incidences of cost of the disclosure accounting process and other barriers. Given the size of the effort that is implied, we don't think it's fair to impose the entire cost on the single covered entity to finance this rework. We would suggest that these costs be distributed more evenly or spread out across a broader range of market participants. At the very least, maybe a requirement that any vendor offering a qualified, certified EHR would have to upgrade existing products and offer products that provide the required reporting functionality and storage of reports in order to maintain product certification. This is more easily said than done. For physician practices that have not yet adopted EHR it's highly unlikely that cost effective reporting, tracking, storage features are today readily available or implementable by 2011, which would be their compliance target. For those of us, who've adopted, we have a longer window, if you will, until 2014. It still means that some of that work, though it might be spread across the vendor organizations with whom we contract, would still require a lot of retooling for the legacy and homegrown systems. While we don't want to whine and grown about this, we would like to simply make the point that this is a non-trivial cost that's competing with other really necessary upgrades and enhancements to clinical decision making at the point of care.

We also would like you to take into consideration again what it would mean to exchange healthcare information between covered entities within an organized healthcare arrangement. We're essentially a group of covered entities working together to provide treatment under contract.

Finally, I'd like to make some points about the meaningful use provisions as articulated by the HIT Standards Committee and we would respectfully suggest that further refinements be made to the provision regarding privacy and security. Specifically, we recommend that the measure, which uses a confirmed HIPAA violation as the basis for measuring privacy and security protection for the EHR be revised or eliminated. We believe that this measure bears no direct relationship to privacy or security protection of an EHR that exists today or that will exist in 2011, the compliance target for this measure.

The existence of a resolved privacy or security violation settled by OCR may arise from a variety of circumstances completely unrelated to the underlying type of security in the EHR. At the very least we suggest alignment of security certification requirements for the EHR as suggested elsewhere in the Standards Committee and its workgroups. The work of the HIT Standards Committee, together with the Policy Committee may usefully coordinate efforts to consider the applicable security standards, both

within the EHR itself and with regard to the exchanges or interoperability. We believe that the focus should remain on the objective security measures and attributes of the EHR and supporting technologies and not on the administrative or management systems that implement the privacy and security compliance regimens for the covered entities.

That concludes my remarks. Thank you very much for your attention.

Steve Findlay, Senior Healthcare Policy Analyst, Consumers Union

Thank you very much, Robin. Questions? Paul first and then Gayle.

Paul

Thank you to the panel. I think their richness of the differences gives us an ability to probe further. In fact, what I would like to do is just reflect each other's comments to give you the chance to respond to each other. For Bob, you heard both, Robin and John Houston actually and Neal say that there is a lot of information that would be in these audit trails, most of which wouldn't be intelligible to most people, including some of the providers. For Robin, you heard that Bob raised there were some incidents that Kaiser had to respond to from the new California law, which would not have been possible if there weren't accounting, because those were inside uses. So maybe you could reflect on each other's comments in that way?

Bob Gellman, Consultant

Well, I'll make a couple of comments. With respect to the numbers of requests that Kaiser has gotten for accounting, if Kaiser would like to get more requests I'm sure I can arrange it by putting out a suggestion for people on the Net; that they should exercise their accounting rights. But there is a reason why people don't exercise their accounting rights. First of all, a lot of people don't know about it. Secondly, the accounting records that are required by HIPAA today are useless. You don't have to account for uses. You don't have to account for disclosures for treatment payment and healthcare operations, so for most people there's not much in the records that's worth asking for.

On the other hand, if you go back and look at what's happened with people getting access to their own record, before we had electronic records at all requests were relatively unusual. Everybody didn't ask for their records. As soon as records became electronic and other things could be done with them there was an explosion of interest in records and the same thing will happen with accounting if they are made available.

In terms of the costs of accounting provisions, I think cost is an issue and I don't dismiss it lightly, but I want to know what the marginal costs are if I give you enough time to implement a new requirement. I'm willing to wait a fair amount of time before you have to comply, possibly as long as five or ten years, and I want to know what those costs are as a percentage of all of the costs of computerization.

The last point that Robin raised about the disclosures to organized healthcare arrangements, I've solved that problem by requiring that all uses be accounted for, so trying to decide what is or isn't a disclosure is no longer a concern. I'm not sure you like that answer, but it's a solution.

Robin Omata, Lawyer, Kaiser Permanente

With all due respect to your framework, I mean I think that what's also lacking here is a fact based decision making process, so you're asserting the number of issues or levels of consumer demand that I haven't seen really documented in national surveys and regional surveys, whether they be based on access to healthcare records or disclosures or uses. So I think that the usual caveat, more research is needed applies here.

But also, I think we don't really trivialize or dismiss the need for accounting. I think that as the information is digitized and moves more extensively that, yes, there needs to be a system in place to do that. I think that the window of time and the manner in which that's imposed, I think, is at issue as well. But I do think equally there is the question of the cost benefit equation when many other investments are required and needed equally. For that I think we do have other competing requests, which are documented, mostly

within our medical system to improve and upgrade reporting systems. So I think we don't at all dismiss the seriousness of providing for our patients' records and traceable pathways how their information travels. At the same time, I think we don't want to over burden the system with something that is of interest to, from our accounts, 0.00004% of our membership.

Speaker

We share your results exactly. We collect 130,000 patients a day around the world and we probably get one, if that many, audit requests a month, so I agree. I mean one of the problems with audits for us is the amount of data we have saved in our clinical data repository that is nothing more than audit trails is terabytes of data. I just wanted to ...

Robin Omata, Lawyer, Kaiser Permanente

Also, just to step back a little bit and say what are the remedies really for patients, I think that stricter enforcement of existing HIPAA would go a long way. I'm not asking you for immediate audits by OCR or the other regulatory agencies, but to the extent that patients do not feel well served by the existing regulatory framework may be a reflection of the absence or the lack of attention to serious claims that Paul brings forth. So I think the additional enhanced enforcement provisions of ... provide for civil criminal penalties, which are significant, and I think there is also more skin in the game because patients may benefit or may receive penalties or the civil damages when a claim is resolved, though that still needs to be defined by the regulations, but I do think that accountability is important. Transparency is important. We don't dispute that in the least. I think it's really a question of methods and the serious attention to the costs.

I think, obviously, the committee has a very, very serious and almost imponderable level of issues to resolve and one of them has to do with the prioritization of the issues technically, as well as in policy and also to assign values, whether they're costs or priority of attention, but I don't think that nationally we cannot look at how things are going to impact the system of care and where those costs ultimately go. So they go to Kaiser Permanente. They end up in the patients' costs, whether it's in the premium or the co-pay, so by layering on added compliance burdens that may not really result in any improvements in direct care I think is not really a great service.

Bob Gellman, Consultant

I just want to make one comment. I mean I think the different points of view have been well put out on the table. Congress said, "Do more accounting." That's what they said when they passed Congress, when they passed the Privacy Act of 1974 said, "Do accounting."

I was the principle house staffer for the Privacy Act for many years and I kept asking agencies, "Is this the problem?" Nobody said that it was. Whether the records are used or not by patients isn't always the test. The records are important, as you see, there are healthcare entities that are doing accounting on their own motion, beyond the requirements of HIPAA, because they need it for their own protection, for their own liability, for their own controls. There are lots of reasons to do accounting for disclosures and uses.

David Blumenthal-HHS/Office of the National Coordinator for Health Information Technology

Other questions? Do you want to move on to our next question? Gayle.

Gayle Harrell, Former State Legislator, Florida

Thank you very much. I think we're getting to the heart of the issue right now. I think I can tell you as a former elected official that this is a critical issue right now. It's cost versus privacy accountability, cost versus the patient's ability to track what happened to their record. I can tell you the public out there may not be requesting their records right now, but as we move into and as the country moves into the level of EHRs that we all hope are out there, this is going to become extremely important. People want to know that the system is accountable and they don't trust government. They don't trust having their public, their very, very private, sensitive information in their health record getting out and being public. This is such a personal issue for most people that I think yes, it may be expensive, but I think we have got to make sure that we make that privacy and security the foundation of anything we do.

We talked about accountability. Without having audit trails, without having documentation you have no accountability. If you want to know what happens at the end of the day and who is responsible you can say, "We need enforcement," but you need documentation to have enforcement.

I think if you're going to say you want to exempt disclosures, one of your recommendations to exempt disclosures as defined in the HIPAA Privacy Rule between parts of a single, organized unit, if you're not going to have that document, if there's not documentation of that audit trail if somebody turns around and says, "Who is responsible for releasing my private information," how are you going to find out how it happened without that documentation? People want to know that there is accountability in the system. They're very reluctant to go down this road to start with, but if you do away without this basic requirement I don't believe people will allow their records to be shared anywhere.

Robin Omata, Lawyer, Kaiser Permanente

Well, thank you. I think we have to distinguish between the audit trail and the disclosure accounting. So audit trails exist for all electronic transactions. The ability to then aggregate that up into another level of reporting to an individual to make it intelligible as to what does that really mean? That transaction went from this machine to that machine for these kinds of purposes I think is really what we're talking about. Because of the volume of transactions that occur, let's say, for this organization about 80 million transactions, which refer to the encounter, to the lab results, back and forth, the treatment, the payment, the settling of the payment, the additional request for information on the radiology. For those 80 million transactions there are electronic trails. It's bundling and connecting them to a report that then is stored for Mrs. X and tells this person essentially all of the electronic points at which the information went back and forth from our organization would be what we would be now producing.

I'm not sure that that really reassures you, but I do have to say that already we do have audit trails for all transactions. Whether that in itself satisfies the disclosure accounting requirement may not be sufficient for what Bob is talking about. I think that it is questionable what that meaning really would be for the vast majority of patients.

Now, we can understand that patients, who have a very sensitive condition that our electronic health record already segments many parts of the record for psychiatric care, for other mental health care, for substance abuse treatments, as well as HIV, other conditions that might be required to be segmented by state law, as well as federal law. To that extent I think one must feel somewhat reassured that the information is really hard to get at unless there is a medical need to know that information or for which that information must be put in transit in order to settle financially the treatment relationship. But I think that's where I would call for more review and study is to say of the 100% of transactions, the 80 million transactions, which transactions might be the most sensitive? What are the characteristics of patients who do or who would ask for this information? Is it really a very specific subset for which we could have more knowledge in order to usefully collect and store disclosure accounting on? For Bob's observation, perhaps there are some uses for some patients that are very, very sensitive that they want to have, but for the vast majority of folks I'm not sure that it's really meaningful and it's a huge encumbrance on the overall capacity of the system.

David Blumenthal-HHS/Office of the National Coordinator for Health Information Technology

Mark.

Mark

... of what you were saying, Robin. The costs, I think, are quite high. The need within our own system has been almost negligible, if at all. The question that I have, and it's probably just a general question, is it almost seems like we're treating all disclosures as inappropriate disclosures. As a technical person, it's far easier for me to implement something that says these are inappropriate, log those and do an accounting for those. But when you say all and you leave this very broad spectrum it causes us to collect a tremendous amount of data. It puts a huge administrative overhead on the organization. I just would agree. I don't think the value is there or at least needed by the members and patients in our area.

David Blumenthal-HHS/Office of the National Coordinator for Health Information Technology

Other questions?

Speaker

... whether anyone in our group has done qualitative research with consumers about both the types of consumers and the types of disclosures or transactions that are most likely in a future state, to Gayle's point, for the public to want to receive disclosure summaries of. Is it possible for us to imagine reverse engineering from a better understanding of consumer requirements to a set of internal technical requirements that would support those. Probably what I'm thinking is if the audit functionality becomes more uniform across all of the vendors then one could imagine a set of extraction and reporting programs that sit on top of those and those are fairly dynamic as long as every provider is capturing the underlying audit data in a systematic way.

Gayle Harrell, Former State Legislator, Florida

It's possible, but that also would require a high degree of granularity to get at, for example, HIV tests or blood test results for other things. You'd have to drill down even further into the information and the purpose for which it was collected and sent.

Bob Gellman, Consultant

If I could make a comment? I mean it sounds to me like from what Robin said the accounting records already exist. It's only a matter of translating them into a more useful form for patients. I recognize that there may be some things that can be done there. I would think as a technical matter; and I stand to be corrected; it's easier to account for everything than to try and make decisions about accounting for some things rather than others because you're going to have criteria that are simply not going to work as neatly as you would like in the real world and there are going to be questions about whether we have to do this or whether we have to do that that are going to be done wrong.

David Blumenthal-HHS/Office of the National Coordinator for Health Information Technology

Richard.

Richard Onizuka, Director, Healthcare Policy, Washington State Healthcare Authority

Very interesting, only to be surpassed over by Deven and Dr. Phil. This is an issue though that we were speaking somewhat about this morning, Jodi. I was hoping that it was the one I was referring to is related to a white paper where I believe our committee needs to be somewhat more informed as to the intent of our specifics of ... around disclosure, because I do believe it's not as simple as you might think. I believe that the majority of providers of systems today do not include this capability and would, in fact, have to re-architect their systems in order to comply, which that be the case, so be it, but it does have a cost and a timing aspect to it. So one of the things; and there is a cost value issue; I think that we would want to know some more direction on this issue to be informed, because it may cause us to go back to our workgroups that focus primarily on meaningful use and maybe have to look at our certification rules to our providers' solutions that they might have to provide additional capability in our out years. So I do think this has lots of implication, not only to society, but also to the work that we've already done here this morning.

Bob Gellman, Consultant

Well, I don't know what the availability of software in this area is. It's clear there are going to be a lot of software changes over the next, what, decade? I don't know how long this is all going to take. If you give people enough lead time to do this it will not be that big of deal. I look around the Internet and I see Internet companies that are tracking every specific activity of individuals, every Web page you go to, every time you click on anything, the cost of storage today for computerized information is as close to zero as it can get and it's getting cheaper all of the time. Companies maintain information in the hopes of extracting a minimal amount of value from it much later on simply because it's easy and cheap to do. I don't see why it's any different in this area.

Unidentified Speaker

Excuse me. Just one follow on for Dr. Blumenthal's ... the one question.

Gayle Harrell, Former State Legislator, Florida

A follow up.

David Blumenthal-HHS/Office of the National Coordinator for Health Information Technology

A follow up. Thank you, Gayle. Not to debate the issue as much as the reason I asked for that clarification is because the intent of ... also came with the intent of a formula for reimbursement to providers for the implementation of these programs and this goes to maybe the definition of extent that this kind of cost was considered within the payment formulas for what we're talking about. Certainly, the technology exists to do it, but this debate about cost value is the critical one. The technology exists today and what I was seeking to get informed on is what was the intent of the law, of the legislation that we're dealing with today, because they don't tell us the extent we're going to go to and then the question is going to be in this day of reducing costs, which I believe goes to what Kaiser is doing within an integrated delivery system is the reason they're able to deliver cost effective care as they challenge every decision like this in order to do so. It's been pointed out as an example of a very cost efficient healthcare system. All I want to make sure is that we balance this with reimbursement and then direction to our suppliers. That's the comment.

Speaker

Judy.

Judy

... you talked about expense to go through all of the audit trails that are there, but really won't make sense to the patient because there are too many of them and they're not tied together in a way that the patient can interpret. I think there are several kinds of expense. One is the people, as you said, to do that. The second is the money. The third is the storage. The fourth that I want to mention is the development. I know we get huge, huge numbers of requests for development that will improve direct care to patients. We're always short of programmers, because the United States is almost 100,000 programmers short every year according to our computer science department because we don't produce enough programmers. So it does become a question of where do you put your priorities, on the direct patient care or on this.

What I wanted to comment on and get your opinion on it was sometimes we look for technical solutions when that's not it. Is the solution to this, if it happens like you said, Michael, once a month given all of those visits, to have a person who is trained in how to read the audit trails so when the patient shows up who has those questions the person can sit down with the patient and walk through with it and interpret it for the patient rather than trying to do it with computer technology?

Robin Omata, Lawyer, Kaiser Permanente

That is not an option we would choose, both because of the enormity of what's actually suggested by the requirement and that's why we're requesting further definition possibly to re-scope our requirement, our obligation. It is possible in a smaller system, I think, to do just what you're saying, but our organization is rather large and we probably would not be able to justify that person's slot given the few numbers of requests that would occur each month.

Judy Faulkner, Founder, Epic Systems

I didn't think it was a 100% job.

Robin Omata, Lawyer, Kaiser Permanente

Right. But I think, not to be facetious, what is asked for is to do 100% accounting on everybody and to store a report on everyone. I mean I think we're not asked to only do that for people who ask for it.

Bob Gellman, Consultant

If I could respond to the point about the records won't make sense, I think all of these records will be computerized. I think it will not be that difficult to take the records, run them through a program that will explain to people, summarize them, run them through something that says who everybody is and what their function is after the fact when a request is received. Just to make a point I made before, Congress

already said, "Do more accounting." You know? They said, "Whatever is being done today isn't enough." They want accounting records for treatment, payment and operations for on-line health records. That's not a question that remains to be debated. Congress said, "More accounting."

Now, I'm suggesting going beyond that. How you do it and how it's paid for and everything else are all certainly legitimate questions, but there is clearly a political demand for more accountability in this system.

David Blumenthal-HHS/Office of the National Coordinator for Health Information Technology

Jodi.

Jodi Daniel, Director Office of Policy & Research, ONC

I have only one question and since I work for David I'm going to stick to the one question rule. My question is for ...

David Blumenthal-HHS/Office of the National Coordinator for Health Information Technology

Two follow-ups allowed.

Jodi Daniel, Director Office of Policy & Research, ONC

My question is for Robin Omata. It seems to me we're talking about audit trails versus accounting. It seems to me, from what I've heard from you and from prior testimony that audit trails are routinely done in order for the entity's own security activities. The question is it seems to me that the audit trails, there is a lot of data and the accounting is to try to turn that data into information that's digestible. That's what I think I'm hearing you say is that that's where the expense comes in taking the data and turning it into information. So my question is where is that greatest expense? Are there particular parts of the accounting that increase the expense or make it very difficult to do this, either because of the workflow that involves the amount of information that's being captured, the translation? I'm not sure. Where is the biggest pain point in turning that data into information that ...?

Robin Omata, Lawyer, Kaiser Permanente

We would first have to create a major project, which would scope the entire effort. I think in actual human resources it would be in the reprogramming or the programming anew to identify and trace and then bundle all of the sources of the information that are going out and then to assign a new English language, plain language explanation as to what that meant, but here again, I would suggest that the granularity of the information that's even available in the auditable trails may not really give a lot of satisfaction to the individual. That is yet another conundrum; that we're not asking for clarification for the sake of it; I think we're really asking for clarification to make sense of what really would be useful to the patient. But going back to your question of where is the biggest expense, it's probably two-thirds in the actual development of the code, but the research on front-end and back-end to make sure that we're getting all of the right trails and that the output in the final analysis, some intelligible report would be the remaining one-third of the work.

I do think though that this is really an untested area. Just stepping back as a consumer I think yes, I would like to know where my information goes. I probably know where it doesn't go when I get to the place that I'm going to and it doesn't show up. That doesn't really happen to me very often in Kaiser, but I do think that outside of our system that might be a concern. It's probably not good enough to ask on an exception basis to only ask for that report then for things that don't get to a certain place, but I do think that what Bob has said before is that you probably don't want to work on an exception basis anyway, because in order to find those exceptions you have to track everything in the first place.

I do raise a fundamental question of what is the real value of this. I think that as you define the other parameters of the information highway, the NHIN, the parameters of security for the EHR, I do think one has to say fundamentally what are the accounting trails that consumers must have? Out of that where does this particular requirement fall? That it's more than just a deep dive into the healthcare records of the hospital or of the physician. It's the continuum of where that information is going and the absolute or the refined information that makes sense to the patient. I think to define first what goes on inside of the covered entity and the accounting per HIPAA might not be the first place to start. It may be the first place

to start because of the legislation, but I think that's why we're asking for more definition in line with the other issues that you're thinking about, which are really focusing and defining this continuum of information flow.

Steve Findlay, Senior Healthcare Policy Analyst, Consumers Union

Thank you. I'm sorry, David. Go ahead.

David Blumenthal - Department of HHS - National Coordinator for Health IT

I was going to say that we do have to wrap it up.

Steve Findlay, Senior Healthcare Policy Analyst, Consumers Union

Yes. Yes. Art, is your question pressing or ...?

Art Davidson, Director, Public Health Informatics at Denver Public Health

It's relatively short.

Steve Findlay, Senior Healthcare Policy Analyst, Consumers Union

Very quick and very quick answers both, because we're out of time on this panel.

Art Davidson, Director, Public Health Informatics at Denver Public Health

I see the point in your statement about focus on standards for security and privacy and not using the meaningful use criteria that we've proposed adherence to HIPAA or having some unresolved conflict with regard to HIPAA. What would you say that we should do if someone has an unresolved conflict with HIPAA? How might that be incorporated or not in your suggestion, Robin, that we just focus on what the Standards Committee is proposing, very quickly?

Robin Omata, Lawyer, Kaiser Permanente

Well, I think it goes back to the enforcement authority of OCR and other bodies that they should step up that activity and make it more swift. The current regimen is not very timely and it doesn't seem to be very transparent itself, so I think that needs a look at, as well as more attention to the overlay or the overlap of this committee's responsibilities and OCR's future responsibilities.

Steve Findlay, Senior Healthcare Policy Analyst, Consumers Union

Thank you. David, do you want to get just one last very quickly?

David Blumenthal - Department of HHS - National Coordinator for Health IT

Very quick. Yes. This is really more of a comment than a question. At Partners what we've done for at least ten years is to provide a report pretty much like what Bob described, which basically let's the consumer tell who looked at their record and what things they looked at. That has been very satisfying to patients. I'm not technical enough to know what was involved in actually doing the programming around doing that, but it's worked really very nicely.

Steve Findlay, Senior Healthcare Policy Analyst, Consumers Union

Thank you. Thank you very much, Bob and Robin. Very good testimony. Appreciate it.

Paul Tang, Internist, VP & CMIO, Palo Alto Medical Foundation

Our last speaker/witness/testifier is a member of the committee, Latanya Sweeney, who is going to talk about technological solutions to privacy and security problems.

Latanya Sweeney, Director, Laboratory for International Data Privacy

... very quickly also. Mark insisted. Anyway, thank you very much for giving me this opportunity to address you. When we were putting together today and we thought about what the panelists would probably say there was just this kind of gloom that happened at least on my end of the phone; I could sort of feel it on the others; about oh my, God, what's going to happen at the end of that day. What's the direction to give hope as opposed to just so much problems and if you try to drill down in like the one that Robin and Bob just had you have to make decisions, but those decisions affect lots of other things. How

do I unravel it? How do I give some content to it? That's what I thought I would address. My short answer, for those who have to leave right away, is through technology design. Let me say a little bit about why I say that.

I think most of you know me, but a quick explanation of what I've done: I've spent a lot of time exposing fallacies in privacy mechanisms, what doesn't work. In fact, in the back of my statement I gave a list of just those related to just HIPAA, but they go across many other domains as well. So if I get really good at sort of learning how you can take innocent looking data and learn really sensitive information from it then the next question is how do you actually control what can be learned? The flip side of what I do is actually how do I prove that privacy is protected. So for every identification experiment that gets a lot of press, there is also a lot of work on the other end of the coin about how do you make guarantees about privacy protection. I've done that in lots of forms, from surveillance to video work, as well as in medical privacy as well.

What is it that I could say to you from that experience and doing that for several years? What's the biggest lesson learned? What it is, what I've learned is that the issue of stakeholder concerns, which isn't just privacy; Gayle, a couple of meetings ago brought up the liability of providers. There are a lot of other stakeholder issues. Recently we were just talking about affordability. All of these things that can be show stoppers actually need to be considered during the technology design. That's where the sweet spot is on solutions. If we don't do it, what normally happens now is we build a technology. This is not us in healthcare; this is just us as computer scientists. We build a technology. It's not quite a proper fit for society and society is left with either the take it, leave it or try to mend it. You either get the benefits or you lose the benefits if you want privacy. There always has been this tug of war, but that's really unnecessary. It's an unnecessary situation that we find ourselves in because if the technology is actually developed with privacy concerns in it, putting the privacy concerns in are often extremely trivial on the front end and really, really painful on the back-end and the ones on the back-end aren't very nice options. They're usually policy, which operates with a big hammer and a crude pin and they tend to be horrible solutions. They're not elegant. They don't give us fine grain control, all of which would be possible from within the technology.

That's why I say we should focus on technology design. One of the things that bothers me, I'm worried about is how do you take what we currently see out there, the standards, the approaches, best practices and how do you actually build on it. There are some problems there, because if we just sort of take what's out there and just sort of say, "Yes, I approve of that and I think we should accept all of these architectures that are out there that show some sign," then in some sense what we're going to do, they're not really made to fit together in a national infrastructure and a lot of the solutions that could go away in a national infrastructure won't. Actually, you're just going to create more stakeholder problems.

I'll give you some examples. Some examples out of privacy is just sort of saying, "You know, we're going to use encryption," just sort of ad hoc-ly saying, "We're going to use encryption to link records of a patient so that we can know which record belongs to which other patient when it's de-identified." Well actually, it turns out encryption has vulnerabilities used that way because there is a shared key. The fact that it's used by one group or one kind of data is actually a good thing for society because you don't really want to use that model on a national level across all of the data, especially in light of many other, better cryptographic solutions. I use that example to say we have to be a little careful to think that best of grade of something that's different than what we're trying to construct is going to get us there.

I'm also worried that the existing standards and practices are just not coherent and they don't provide the functionality to realize the vision of a national infrastructure. A great example of that is the simplest problem of all and that is you've got these timeless collections of records. I just want to know where Alice's records are. How do you answer that question? Alice is in some random city and she wants to know and her doctor wants to know where her records are. The fact that we can't address that, that's not good. The reason is if you think about all of the issues that came up today and I told you, "You know how we're going to address it? We're going to have one big central authority, who is going to capture all of the data, so whenever you want to know where Alice is you just contact the authority and that authority will

give you Alice's information." That changes every discussion we had today. The issue about burden; it immediately tells you where the burden is. A lot of it shifts now to the central authority and so forth.

If I alternatively told you the opposite, there's not going to be a central authority. Every local provider, every provider, who wants to, is going to keep their data on their little PC or on the hospital system or what have you and we're just going to make sure our network is robust enough to answer the query. Now you have the question of how do you know where Alice's data is? Isn't there a role still for central authority to identify? Maybe it's just a master patient index. That again changes all of the discussions today, but that also still leaves us with a serious privacy problem. What does it mean for an authority to have a master patient index? That's actually how we got the HIPAA Privacy Rule for those of us who were around at that time, remember?

So technology design radically changes. Architectural planning will radically change all of the discussions today. If you put on the table five different designs and then you ask all of the speakers to come back again, now what happens is they can tell you why they like that part of that design and they hate that part of that design. That's a really great discussion to have. That's the discussion I want us to have if I had my wish list. It's your call.

I said, "Okay, how do we get there?" Because the problem is those five designs, they don't exist. They're not there. So I know that CMS has an RFI out asking industry, "Help. How would you go about building one of these things for Medicare?" They're going to get lots of answers, but I don't think that's going to get us there either, because industry is going to answer by leveraging what they already have. They're going to leverage existing practices and they're not necessarily going to know about other technologies from other areas. So I think it's a good step, but I don't think it's really going to get us there. The question is how can we deliver that.

So after me ranting and raving for months about this many times to Judy, a group of us academics actually decided that we could help here. We could actually make a difference in the sense that if we brought industry and stakeholders together, our goal is not to solve a problem. That's the job of ONC and the Policy Committee. Our goal is not to build technology. That's Judy and many other companies as well. That's their job. Our goal is to make sure that the technology and the decisions that are made are really well informed. That is can you put together pieces of not just one answer, but five answers with interoperable pieces so that one could actually have a discussion on which you can see the policy implications.

So we did commit ourselves to this sufficient that we actually have a name. We call it the Advanced HIT Project and it's going to be launched on Monday, AdvancedHIT.org. We bounced it past a few people, some of which are sitting at this table. Everyone was very enthusiastic, including the industry partners, who understood that the outcomes of these things are just white papers. They're publicly available because we'd like the public to be involved in comments and anybody else who wants to participate. The original research foci are at Carnegie Mill and Harvard and MIT, but we seek out the best people, so if we need to help the economists and the best one for this particular job is at John's Hopkins we'll be reaching out to him to help us so that we can have the best informed analysis.

So my goal was to try to leave you with hope and if I couldn't leave you with hope, with some idea of maybe we should look at architectural designs.

Paul Tang, Internist, VP & CMIO, Palo Alto Medical Foundation

Well, thank you for your statement and, B, your commitment to working on this problem. One clarifying question: The problem you're working on and trying to design an improvement for is the privacy and security problem. Is that correct?

Latanya Sweeney, Director, Laboratory for International Data Privacy

No. When I say that my lessons from privacy are very much really that the best solutions are in the original technology, so if surveillance has a problem the best answer is not a privacy add-on. The best answer is to change the way you do surveillance so that it has privacy protection. If Twitter is doing

something that is having privacy problems it's Twitter that has to be changed. It's not an add-on per se. So the idea is all of these discussions change depending on what kind of notion you have for the infrastructure. There is a lot of function that we see in the vision for the infrastructure that no-one actually knows how to do. I mean people can beat their head up and people can spawn ideas off the cuff. I spawn too. Leave the data at the lowest level and put the data in one big aggregate level. Those are two models, but how good are they? How robust are they? What stakeholders would scream about what and be legitimate that we could actually quantify and so forth, because it's going to change all of the privacy issues? Some things might require what becomes the issue changes. Even this issue of the audit trail would change.

David Blumenthal - Department of HHS - National Coordinator for Health IT

Yes. Rich.

Rick Chapman, Chief Administrative Officer/CIO/EVP, Kindred Healthcare

Just a point of clarification, Latanya. I'm too a supporter of architected solutions and certainly we like to have more innovation, but I'm somewhat confused. Are you talking about this technology that would support a national exchange with identified data?

Latanya Sweeney, Director, Laboratory for International Data Privacy

I'm not talking about a technology. I'm not talking about me building any technology. I'm not talking about me being a part of any solution, operational solution. All I'm saying is that I wish today the conversation had been a different one. I wish that there had been a meeting that said, "Hey, here are five ways we could design this. Here are the features that we really want off of whatever your vision is for this national infrastructure. Here are the features and functions we expect. Here are five vendors or five groups who represent five different ways we might construct that."

Then we get to sit back and then we could ask all of the people who testified today, "How do your privacy concerns map into each one of those architectures?"

Rick Chapman, Chief Administrative Officer/CIO/EVP, Kindred Healthcare

Okay. Thank you.

Latanya Sweeney, Director, Laboratory for International Data Privacy

So my goal is to help us get to the five.

David Blumenthal - Department of HHS - National Coordinator for Health IT

Christine.

Christine Bechtel, VP, National Partnership for Women & Families

I have a couple of questions. First of all, let me say this is really fabulous food for thought and I really appreciate the thought leadership that you're bringing to this.

One of the things that ONC did a number of years ago was, in fact, this consortia work that they did to test what I presume would be architectural designs. If memory serves, I think IBM did one that was a little bit more like a big data warehouse and other folks, CSC, Accenture and others did different models that were a little bit more federated. So my first question is clarifying is what you're talking about looking at those types of architectures and trying to identify some options and some things that we could say if we're trying to accomplish these policy goals this is what it means if you look at this architecture design versus that? So am I first on the right track?

Latanya Sweeney, Director, Laboratory for International Data Privacy

Yes.

Christine Bechtel, VP, National Partnership for Women & Families

Okay.

Latanya Sweeney, Director, Laboratory for International Data Privacy

But not those architectures per se, because five years ago in the world of computers is a long time ago.

Christine Bechtel, VP, National Partnership for Women & Families

Absolutely. Okay. So that makes a lot of sense. My second question and then I have one comment and that fits within my three rule, your three rule; my second question is can you talk about the issue of data use? I think what we heard a lot about today, whether the discussion was about consent or whether the discussion was about audit trails, what I think a lot of it boils down to is how is data being used and really focusing on patient and consumer concerns about downstream, well downstream uses. Can you talk about how would architecture design impact the use of data? I mean I guess where I'm getting stuck is I think we still; and I know you would agree; need a policy, but can architecture design get to a policy or does it really just need to be built to follow a policy around data use for example?

Latanya Sweeney, Director, Laboratory for International Data Privacy

Well, I think the meaningful use matrix is a really great guideline about this is what we want to realize. I think it paints the vision very clear, but the truth is in my mind I keep saying it's kind of etc. There are rows in the matrix that aren't visibly in the matrix, but you hear them in the discussion, but they're not visibly in the matrix. So this gets to this notion that there are more uses than just meaningful uses about it.

The way architecture plays in that is really interesting. I can't imagine any complete solution that doesn't enable about a \$1 billion industry of data analytics that's going to want to work on top of that. There already is a data analytics industry in this area, but having an infrastructure will enable it. Is that a good thing? Is it a bad thing? Are those just acceptable? Some of those uses resonate with our ability to do the outcome measures that show up in the meaningful use matrix. Some of those uses might be other ways to save money, like identity theft, for example, medical identity theft. But those are all policy decisions and that might be part of what you think of when you think of the architecture, so that particular example of use is one I think all of the architectures will probably have.

Christine Bechtel, VP, National Partnership for Women & Families

Okay. So my very quick comment, but very important one, is that I think that we have to do, as a committee, some real work around identifying the set of policies or at least a beginning set of policies that can move us forward. If we can have the opportunity to then just ... policies up against different architecture designs, fabulous. But I want to be clear that in our conversations with Congress, well before HITECH was passed when it was the Wired Act and others, they really wanted to see this committee, in fact, and AHIC before it tackle privacy policies. So I want to encourage us to commit to; and I'm sure that you'll talk more about the future of our work in this area, but commit to crafting what that set of policies looks like, how it builds on best practices in the field, how it builds on the work of Markle, the state of Minnesota, all of the wonderful folks that we've heard from today so that we can at least begin to have the discussions, again, building on the work that's been done about what the right sets of policies are and then be able to look at how they interact with architecture design. But this is an area that we have been debating and struggling with, as I know you know and others, for years and years. I think it's that this is the next best opportunity that we have to really make some progress.

Latanya Sweeney, Director, Laboratory for International Data Privacy

But can I just push one thing on you, Christine? I agree too, but I think that having the policies discussion in abstraction will lead to a set of policy guidelines that will be far from optimal.

Christine Bechtel, VP, National Partnership for Women & Families

I agree.

Latanya Sweeney, Director, Laboratory for International Data Privacy

At the end of the day they're not going to serve us well. I think the panel before; I forgot who asked the question that led to the panelist saying, "Well, we should start with policy and then have an architecture." Now I'm coming to you and saying we need to work on architecture. I'm not saying you do architecture and then policy. I'm actually saying it's called iterative design.

Christine Bechtel, VP, National Partnership for Women & Families

It's both.

Latanya Sweeney, Director, Laboratory for International Data Privacy

You have to bounce between the two so that you actually find the optimal spot. Engineers call it iterative design.

Christine Bechtel, VP, National Partnership for Women & Families

I completely agree. I think that this committee, as you proceed with us with your work with the group that you have assembled, clearly some of the best minds in the country, we, as a Policy Committee, I think should not just sit here and go, "Wow! We're going to wait for Latanya to do her thing."

Latanya Sweeney, Director, Laboratory for International Data Privacy

Right.

Christine Bechtel, VP, National Partnership for Women & Families

We need to pull together. There are some great people, Deven and others, Joy ... and others, who work with this committee. I think that we all bring wonderful perspectives and it's an opportunity to do exactly that, to iterate, to be co-working together at the same time on both the policies and then bouncing them off the architecture designs.

Latanya Sweeney, Director, Laboratory for International Data Privacy

I'll just say one sentence, two sentences, three sentences because we're under David's rule. If you do that then it actually changes what's important from the architecture. For example, if people were to say in the earlier discussion, "You know what? That's not really what we meant about how we wanted audit trails to work," then that actually might push the work away from some design. But on the other hand, if there's a group that was clear, "No. No. No. This is what we want. We want this kind of accountability," then we'd be knowing that feature. I know that there are a set of principles, for example, that we had talked about on the phone. I assume that those principles would be the kind of thing and beefed up a bit.

David Blumenthal - Department of HHS - National Coordinator for Health IT

Regrettably, I'm going to call the question at this point, because we have to hear from the public. I also want to say that we do have to have some next steps. We don't have time scheduled to talk about it and I'm not sure we're ready to talk about it. We have to, I think, digest the many suggestions and thoughts we've heard today. I do think that one thing we do need to do is put together, maybe reconvene the task force that put this series together and have that group propose a set of activities for the Policy Committee going forward. My own feeling is we can't propose a set of activities that's going to take five years to bring to completion. We have to have a series of short and middle-term and long-term, a menu of things.

Now, the fact of the matter is that we do have a law to implement. We don't have all of the time we'd like. The law assumes that we can get a lot of the nation's providers to be meaningful users by 2011. If we were to decide that none of the architectures that are currently available are correct I'm not sure that would be very helpful to us in the short-term. So I think we are always going to have to move ahead with what's practical, as well as what's ideal. But I think let's put together a group to sit and think about it. If you have a burning desire to be on it and you weren't on it before we'd be happy to entertain that offer.

At this point I think we'll thank you, Latanya. Thank you for the thoughtful comments. You clearly have stimulated us. I don't know if you made us optimists, but you've stimulated us.

Judy, I think we're ready to hear public comments.

Judy Sparrow – Office of the National Coordinator

Okay. This is the public comment portion of the meeting. Anybody in the room who cares to make a comment, please queue up to the mike. Those on the telephone, you can dial 1-877-705-6006. Anybody

in the room who wishes to make a comment, please state your name, your organization and we're asking that you keep your comments within two minutes.

Deborah Peel, Founder & Chair, Patient Privacy Rights

It's me, Deborah Peel. I know I've taken up a lot of your time and I will keep this to two minutes. Congress did intend for outside experts to be participants in the workgroups and to be asked to help with projects. I would like to reiterate again our offer as the leading national representative of consumers interested in privacy, in health technology to help you. Either we would participate or we have many strong members of our coalition, who would participate to bring the consumer perspective on privacy into this process. That's my offer. We just want to help. Thank you.

Judy Sparrow – Office of the National Coordinator

Is there anybody on the telephone? Next.

Joy Pritz – Georgetown University

I'm Joy Pritz. I'm with Georgetown University's Health Policy Institute. I know that this meeting was primarily for information gathering, so there are a couple of pieces of information I'd like to give to the committee. One is that a lot of work on these privacy and security policies has been done by other countries, who have faced the same challenges. NHS, as David mentioned earlier, has pursued one option of how they will deal with health information. We may or may not wish to adopt their solution, but they do have white papers that outline their consideration of the very different options as to how they would implement that and why they reached the conclusions they did, so that, I think, would be a very useful tool for this group to have.

In addition, Canada has had very thorough analysis of policy and security considerations in the Pan Canadian solution. They have almost an abundance of information. It would be worthwhile having somebody comb through some of that information. It's very useful. It is very organized. It has addressed a lot of how you segregate information, including vendor conformance requirements and things of that nature. It is all available publicly on the Internet for free. Thank you.

Judy Sparrow – Office of the National Coordinator

Thank you. There are no comments on the phone. Any other comments in the room? Judy Faulkner.

Judy Faulkner, Founder, Epic Systems

I'm not sure, David, that we're all talking about the same thing when Bob and Robin were talking. You were talking about the audit trails and I think; they can correct me; what they were meaning was not the EHR system and whatever else is in that same package have the ability to have the audit trails that the patient can see, because I think most of them do. I know we do. I think the question, and correct me if this is wrong, is when it goes to LabCorp, whoever sees it in LabCorp, how is that brought back in. When it goes to the insurance company, who sees it from the insurance company? How is that brought back in? I think that was the question. I'm ready to stand corrected if that wasn't it.

David Blumenthal - Department of HHS - National Coordinator for Health IT

Thank you for that clarification or comment, Judy. We should just make sure that anyone who wants to talk on the phone or in the audience is.

Judy Sparrow – Office of the National Coordinator

Yes. There is nobody on the telephone.

David Blumenthal - Department of HHS - National Coordinator for Health IT

Okay.

David Bates, Chief, Div. Internal Medicine, Brigham and Women's Hospital

... there isn't anything in the law that requires you to account you, as a hospital, to account for something that somebody else did with the data. Just to get a sense of the scope of this ...

Paul Tang, Internist, VP & CMIO, Palo Alto Medical Foundation

To figure out where the problem is because I know, just like, David, you're saying your system does and ours does it and I know most of the others do it ...

David Bates, Chief, Div. Internal Medicine, Brigham and Women's Hospital

...

Paul Tang, Internist, VP & CMIO, Palo Alto Medical Foundation

Yes. So I don't know where that depth of problem is then, which brings up a whole new bunch.

David Bates, Chief, Div. Internal Medicine, Brigham and Women's Hospital

Well, we clearly need a working group to clarify all of this.

Paul Tang, Internist, VP & CMIO, Palo Alto Medical Foundation

Yes.

David Blumenthal - Department of HHS - National Coordinator for Health IT

I want to express again my appreciation to all of our witnesses, to the members of the committee. We are going to be continuing to work on this problem. We have a lot of implementation to do. We didn't talk about all of the regulatory work that is being done to implement the HITECH law as it amended HIPAA. There's an enormous amount of work to do in that area, but there also is some additional work. If it needs new Congressional authority we will, of course, have to take that into account as we go forward.

Without objection, I think we stand adjourned.

HIT Policy Committee Public Comments from the Webmeeting

1. Sad to see that they didn't use this to get questions to the committee meeting
2. We continue to hear about the split between an EMR - which is similar to my bank being online and PHR's which is akin to using quicken. In order to achieve a patient centered health care system shouldn't the architecture goal be for a shared care plan in which patients do in fact write to their clinical records - like the 580,000 members of Group Health and millions at Kaiser already do?
3. HL7 has models already designed See HL7 RMES legal committees This team has defined both functional and technical models for CDA privacy processes.
4. We are beyond policy now. The policy is already well defined and not in practice.
5. Key question: WHAT IS THE EVALUATION CRITERIA FOR EVALUATING TECH MODES FOR PRIVACY AUDIT TRAILS?
6. SPECIFICALLY RELATED TO REVIEWING TECH MODELS AND EVALUATING EACH OF THOSE MODELS
7. EXCELLENT PLAN TO ADDRESS THE COSTS OF PRIVACY AUDT TRAIL. THIS IS ABSOULUTELY CRITICAL PATIENT CONFIDENCE
8. Some of us already came up with an architecture
9. Latanya, I agree with you that the technology has to be tamed and customized to solve a given problem
10. Audit trail used to mean comparing data, and then segmented data can be audit easily, like medication. You do audit trail to see whether the patient is allergic to a medication, that is really simple to do
11. If a Technology is the limiting factor, then we can do nothing- maybe it is our perceptions
12. As far as accountability is concerned: I think the technology is given with minimal cost, but the size of the data is a problem, however, the duration to keep the data as Mr. Gellman indicated may help resolve storage problem
13. We continue to hear about the split between an EMR - which is similar to my bank being online and PHR's which is akin to using quicken. In order to achieve a patient centered health care system shouldn't the architecture goal be for a shared care plan in which patients do in fact write to their clinical records - like the 580,000 members of Group Health and millions at Kaiser already do?
14. ONC has to have wait and see attitude until the project narratives from each state is received and learn from it and choose the best
15. All lawyers and policy makes unit to address the root cause of a problem, like, why personal medical data is sought, all the technology in the world cannot make a data more secure
16. According to the new initiative, a primary care provider is not the owner of the data of a patient, the patient can change a primary care physician, and that physician will not have the patient data in its local system, this is possible due to centralized distributed architecture going to be in place
17. Please remember that health care records belong to the patient, will he have the right to withdraw his or her own records, if they choose. Also, should this individual have the right to limit access of specific entities to his or her data
18. Are there systems in existence that handle these types of privacy issues?
19. Would how info from say the MasterCard/Visa transactions system give a start or are there still too many holes there?

20. I am Mr. X, I selected a plan A, plan A requires me to choose a primary provider, expert provider, etc. The IDs of these providers will be in the record under my ID. These providers can access my data using the proper procedure
21. For general use, like ER etc, then we have summary data, which help a provider to know enough about a patient; expert provider will have relevant information in the field they are expert on.
22. To know who accessed what, then the way to go is with a centralized distributed architecture
23. What is the consequence of knowing someone's medical data? Not able to get insurance and not able to get employment? What is policy in this regard?
24. What thoughts do you have in relation to ease of use vs. security? Currently, providers can share information with services like Google Health and Microsoft Healthvault but it requires the sharing and verified of a 16 digit alphanumeric code to establish the link. That alone can cause a barrier of use.
25. Does the law say that a patient can share personal medical data for outside of meaningful use by consenting?
26. When a patient in cancer treatment, is that covered as treatment or not, then the statistical analysis may not need the patient personal data, in this case, do we need consent
27. What is meaningful use of data mean when we speak of insurance firms
28. Sharing is for data sharing with non medical professions, insurance, marketing folks, etc., and access is for data access by different providers for meaningful use
29. Patient record and physical architecture of the system used for that purpose are vital to come up with robust system that can be accessed by different set of providers who are in contact with patient without going through many hops, such as, consent, etc.
30. Are you going to define also on segmented data who has access privilege regardless of the patient's request