Transcript provided by kaisernetwork.org, a free service of the Kaiser Family Foundation[1]
(Tip: Click on the binocular icon to search this document)

Health Information Technology and Privacy:
Is There a Path to Consensus?
Alliance for Health Reform and Divided We Fail
February 29, 2008

[START RECORDING]

ED HOWARD, J.D.: I want to welcome you to this briefing. My name's Ed Howard with the Alliance for Health Reform, and on behalf of our congressional leadership, Senators Collins and Rockefeller, and our board of directors to this briefing on how to pursue the greater use of health information technology while protecting individual's privacy rights.

Our partner today is the Divided We Fail initiative and its four main sponsoring organizations, AARP, the Service Employees International Union, the Business Roundtable, and the National Federation of Independent Business. They've actually given you a little mouse pad inside your materials so you won't forget them. We're very pleased to have this sort of strange bedfellows coalition that's actually much broader than those four groups as well involved in trying to find some common ground on one of the most hopeful aspects of health reform in my judgment.

If you look over the reform plans of the major candidates for president, you see that all of them understand the importance of health IT. In your materials there's a side-by-side that compares some of the leading congressional bills on the topic. You can see by looking over that document that there are some thoughtful, fairly comprehensive bills that address IT issues. But frankly those bills and all of the

---

major pieces of legislation focusing on IT issues are now stalled in one house or another, and from most accounts one of the biggest sticking points, is finding the right balance between making access to patient records easier for health professionals and protecting the privacy rights of the individual patients.

Today, we hope we're going to understand what's at stake from several different points of view, see if there are some areas around which there might be a workable consensus. We need to make sure that patients feel secure enough about their records remaining confidential that they allow reliable, complete information to be placed in their electronic records. We need those electronic health records to get a more efficient health system.

As I mentioned, we're really pleased to have as co-sponsors for this briefing the Divided We Fail group and we've got John Rother, who's the Director for Policy and Strategy for AARP here representing that coalition. John, we're going to hear from you later in your formal presentation on the topic, but maybe you could just say a few words now about Divided We Fail.

JOHN ROTHER: This is definitely the topic that the four lead partners of Divided We Fail wanted to focus on because we feel like this is so critical to moving forward on

---

our shared goals of more efficient, higher quality and safer health care system.

So, Divided We Fail is an effort that was started several months ago to bring issues forward with the public as well as with our political leadership. It was started by AARP, the Business Roundtable and the Service Employees International Union, and then NFIB has also joined as a principal partner. Today we have more than 60 other organizations, everyone from the Consumer Federation to the Republican Main Street Partnership. The effort is bipartisan. We're trying to make sure that we keep the big picture in mind in terms of our ultimate goal which is quality, affordable health care and lifetime financial security. And so today I'll be speaking for the coalition with regard to the issue of health IT and privacy. Thank you, Ed.

ED HOWARD, J.D.: All right, John, thank you very much. And thanks to the members of the coalition for their support and co-sponsorship of this briefing. Let me just do a few logistical tasks here. By Tuesday morning for sure you'll be able to view a webcast of this briefing on Kaiser Network.org. And in a few days you'll be able to view a transcript of today's discussion, along with copies of the materials that you have in your kits at both KaiserNetwork.org and AllHealth.org. There's even a podcast you can download at some point.

And let me just say one word about these materials. In addition to the nice mouse pad that you have there are a couple items of uncertain provenance I guess you would say that I wanted to note. There is the side-by-side that I mentioned which carries no author up front but comes from the National Partnership for Women and Families. And then there's a gray handout that's on the table in the back headed "Health Information Privacy Protections Under State and Federal Law." That comes from the American Bar Association's Department of Health and Human Services project, not from the Department of Health and Human Services. And I'm sorry if there's any confusion about either of those items.

You have in your packets a blue evaluation form that we're going to ask you to fill out at the appropriate time so that we can improve these briefings as we go along. And a green question card that you can fill out and hold up if you don't want to get up and use one of the microphones that are in the audience for you to ask questions directly following our presentations.

So we have three terrific speakers today to help us grapple with these tough questions. I ask you to turn your cell phones to vibrate. I mean really do it. Don't just listen to me say it. I don't want to hear the ringtone that you downloaded last week. And let us get on with our discussion.

Leading off this afternoon is Jodi Daniel. She is the Director of the Office of Policy and Research within the Office of the National Coordinator, ONC for HIT within HHS. Those of you who are not in Washington may not know what all that means, but there is an acronym list on our website. You can sort it out. She's been working, Jodi's been working on privacy issues within HHS at least since the days of the last big privacy law known as HIPAA; there's another acronym I won't repeat the names of. And now she coordinates the health IT policy discussions within HHS. We're really pleased to have her with us today. Jodi?

JODI DANIEL, M.D., M.P.H.: Thank you very much, Ed. It's really nice to be here and to be talking about this topic of health IT and privacy. As Ed mentioned, both of these issues are near and dear to my heart and issues that I've been working on for many years. And I'm also encouraged by the title of this presentation, "Is there a path to consensus?" Because as the speakers discussed and we had a conversation about this, we all agree that there is a path to consensus and we're all committed to trying to reach that consensus.

I wanted to start off quickly by talking about the benefits of health IT because there are— this is not about the

---

technology. It's about health care. And Health IT and electronic health information exchange can enable the transformation to higher quality, more efficient patient health care, and better health. And that's really the purpose here to have that information in electronic form and available anywhere, anytime so that providers can better treat patients. And patients in their designees can have access to their complete health information.

So, I want to just posit how we should be prioritizing these issues. There's two different ways of looking at this in a simple world at least, is looking at the new issues or opportunities raised by health IT or using health IT as an opportunity to reconsider existing policies. And I'd like to suggest that we focus on the former; that we should be focusing on the new issues or opportunities. There are lots of issues. There's lots of difficulty in trying to get to solutions on privacy with respect to health IT. And I think if we're looking toward a path to consensus we should be focusing on the areas that are new where I think we have a better chance of reaching some consensus, rather than trying to re-think some of the issues that have been debated for decades quite frankly.

So with that in mind I want to focus on some of the things that I think are new. There are the capabilities to link health information. This both poses opportunities for

---

better health care and reduced medical errors, and also raises some concerns by consumers who may not want that data linked. There are capabilities to look up patient information so that health care providers could know what other health care treatments the patient is receiving and make sure to coordinate that care well.

There are opportunities for enhanced protections. You can use technology to provide greater access controls by making sure only authorized persons have access to the information and only have access to the information for legitimate purposes. In addition, the technology can allow for audit trails or the ability to see who has accessed the information to make sure in fact it is being properly accessed and that there aren't inappropriate uses or disclosures of the information.

There are also opportunities for greater consumer involvement in their health with health IT based on increased consumer electronic access to their health information. Health IT and health information exchange can allow consumers to e able to collect all of their information from all of their providers in a personally controlled health record that they can see, they can control, and they can provide access to as they wish.

I also want to look at what we already have in place as a foundation so that we can build off of that foundation and

---

focus on some of these new issues. There are both federal and state laws that are in play. At the federal level, as Ed had mentioned, the HIPAA privacy and security rules which I'm sure most of you, if not all of you, are very familiar with. This is the Health Insurance and Portability and Accountability Act. These rules protect health information held by health care providers, health plans, and health care clearinghouses.

There are also specific rules on the confidentiality of alcohol and drug abuse patient records, the Federal Privacy Act, which governs federal agencies that provide or pay for health care. And then there are some other laws that are interesting to keep in mind, like the Federal Trade Commission Act. This doesn't directly address health information protections. But if, for instance, a health IT vendor, like a personal health record vendor or a health information exchange organization puts a privacy policy up on their website, the Federal Trade Commission can enforce if they fail to comply with those stated policies. So there are other levers that we may be able to look at and other laws that may help in providing consumer protections.

Of course there are also state laws in this area, the HIPAA privacy and security rules provide a federal floor and state laws that are more stringent continue to remain in effect. Those laws are important. They also pose some challenges because of the variation among the states in those laws that may pose some challenges for interstate exchange of health information. And we should also keep in mind that there are other types of protections like contractual requirement through data use agreements and the like, or organizations put in place protections of the information.

So what are some of the issues I think we need to focus on? Ed had mentioned this first one, and I really think it is the crux of the debates on privacy and health IT. There's this tension between access and privacy. If you have unfettered access to the information you have privacy concerns that are raised, and if you have so many privacy protections the information is locked down you don't get the benefits of access to the information and improved quality. There's a tension here between these two and I think it's really the crux of the debate that we have and that we have to work through. There's some misconceptions about the existing laws that are out there. And those may lead to some more conservative approaches for how folks apply the law that we need to work through. And there's some confusions about how those existing protections apply in this new environment, in a health IT and health information exchange environment.

And finally there are protections that may not reflect the new environment. At the state level you have prescription

---

laws that require wet signatures or triplicate forms and didn't consider the ability to electronically prescribe which does have great benefits for consumers by reducing adverse drug events. At the federal level we talked about, I mentioned HIPAA, and HIPAA doesn't cover necessarily all entities involved in the health care system. So we have to look at how the protections apply in a new environment.

So how can the government help the health care system strike the balance I talked about, about access and protections? Of course there's legislation and regulation and we have done that in the past, but I think there's also some creative ways that we can assure that there are appropriate protections in place. There is the ability to certify products or accredit entities to assure for instance that there are security capabilities in health IT products and that the entities that are implementing these products have policies in place to secure data and to protect data. We can also use our, the federal government can use its procurement power to assure that anybody who we're contracting with or we have grants with, have certain protections in place for the health information that they hold.

Just to talk briefly about some of the things that ONC is doing to coordinate a nationwide approach. At the state level we have helped formed the Health Information Security and

---

Privacy Collaboration or the HISPC. There's an executive summary of the impact report that just recently came out in your materials. This is really a grass roots effort involving 44 states and territories and working over with over 4,000 stakeholders across the country. It's really helped to have a dialogue about these issues about protections, about variations, and right now we have states working together on seven projects to look at solutions that can work across states in addressing some of the challenges that they have identified themselves.

We also are working at the leadership level with states on the State Alliance for e-Health, which will have its first report out in March of this year. They're looking at policies regarding health IT including protections of information. And will be focusing on consumer involvement, education and protection, accountability, and alignment of their policies in the next year. At the federal level we have the Federal Advisory Committee of the American Health Information Community and a workgroup that's specifically focused on confidentiality, privacy and security issues. They are trying to grapple with these issues at a federal level.

We're also trying to figure out how we can make sure that policies are incorporated into our technology activities, specifically we're looking at consumer capabilities in a nationwide health network trial implementation. These include the ability to exchange consumer permissions enabling consumers to have electronic mailboxes so that they can receive their health information from their providers as well as access logs. HHS is also going to be taking a lead role in the next year in trying to coordinate a broader nationwide approach to some of these issues as well.

So I wanted to sort of close with the considerations for policy development that we're looking at. And we'd hope others would too as they're looking at these issues, first recognizing the foundation of privacy protections at the state and federal level that already exist, assuring that there aren't unintended consequences of policies by considering the impact on patient care that the policies may have, and also by thinking of creative policy mechanisms that can adapt with technology changes. We've seen with HIPAA standards, when we put the standards in place and regulations and then the industry has improved upon those standards and it takes years to make those changes and have them adapted as policies.

So looking at how we can be creative there, building consensus by including various stakeholders and getting stakeholder involvement, and as I'd mentioned at the beginning, prioritizing. So I think we can have a formula for quality health care by having electronic health information, appropriate consumer protections and consumer access to their information, leading to trusted health information exchange so that we have confidence. Patients and providers have confidence that the information will be protected in order to mobilize that health information to lead to greater quality of health care. For more information I gave you our website so you can see some of the other activities we're doing, and look forward to your questions. Thank you.

ED HOWARD, J.D.: Thanks very much, Jodi. We're going to turn next to Deborah Peel, who's a practicing physician and the founder of an organization, Patient Privacy Rights. She's formed a broad coalition, which we didn't list in her slides, but which will be available both on our website and in hardcopy if anybody wants to just email to us. And that coalition advocates for patient privacy and it includes a wide range of groups from across the ideological spectrum; it's a very impressive list. And personally I should note that Deborah Peel was certified last year as the fourth most powerful health care person in the country by Modern Healthcare magazine. So we're doubly sure to enjoy your presentation, Deborah.

DEBORAH PEEL, M.D.: Thank you, Ed. I really appreciate this opportunity to be on this panel and talk with everybody about how we can find a consensus to move health IT forward and protect the most sensitive data on earth which is your health records, information about your body, your mind, and your genome. Let me just say that I come from the ground underneath the grass roots. I'm still in practice. I've been practicing for over 30 years as a psychiatrist and that's the most privacy-sensitive specialty in medicine. And so long before there were computers or managed care or any of this, people came and paid me cash on the barrel head because their lives or their reputations had been ruined.

And so it doesn't take a lot of foresight to realize that if we wire everything together without control over where this sensitive information goes, we're going to see rampant discrimination and really problems with people's jobs and livelihoods as well as embarrassment and problems with their reputation. So what I want to really talk with you about is where the world is now. What kind of a health IT system we have today. And I think— maybe I'm not working this right. Okay.

What we have to start with is what happened to HIPAA. HIPAA was intended by Congress to be a privacy rule, a set of regulations that actually laid out at a federal level for the first time, rights Americans would have to control their information. Some of you may have seen this particular slide. It's been our most powerful educational tool for the media and for policy makers and leaders because it shows what happened.

And I think you'll see in the top box the intent of the statute. The top, box number one is essentially Congress's directive to HHS when Congress failed to pass a federal privacy rule. Box number two is what gave us the privacy present [misspelled?] When President Bush implemented the rule, you can read that sentence, it's clear, crystal clear, that each of us have the right to decide when our information was used and disclosed. Box number three was never reported by the media. Never reported. And Congress really didn't understand that HHS essentially completely subverted its intent when it amended the privacy rule.

Now the privacy rule is thousands of pages. It's not astonishing that people missed this single sentence, but this is the key sentence. You have to think about it. What it really says is that it's no longer your choice about when your information goes out. The providers, the covered entities decide, do they need your records and which ones for payment or for treatment or for health care operations, and health care operations essentially means any business purpose. This is a little more of the direction of what Congress intended the rule to provide. The rights an individual should have and procedures to exercise such rights. Today, we do not have any opportunity to exercise our rights under federal regulation to control our health information.

Okay. Again, I come from the cottage part of health care industry, doctors sitting in a room with patients, in my case one patient. And we're forgetting that the only reason, the absolutely only reason that anyone comes in and trusts the doctor with anything is because they think that their information is going to be protected. Doctors take the Hippocratic Oath; swear to protect their patients' information. But they're not able to in today's world. The point is, and I guess I'm being long winded about this, but the point is if the patients don't believe that their information is going to be used to help them and not harm them, they're not going to make these disclosures. They're not going to come in. They're going to lie. They're going to omit. And what we're saying is there's no reason to have health IT without privacy. Privacy is not an obstacle.

This slide breaks every rule and I'm sorry. You can't really read it. But the point is to give you a feeling for how many millions of entities and individuals can see and use your health record, thanks to the fact that HIPAA was gutted. The first zone surrounding the patient is designed to represent the providers and the covered entities. Everything from a solo doctor like me to Hospital Corporation of America, to self-insured employers, and on and on, all can now use your records without your knowledge retroactively, even if you object

---

because HIPAA was gutted and has given them this authorization to use your records. Beyond the covered entities, of course, there are business associates which covered entities can share your information with, everything to transcribers in Pakistan. And lastly, Gramm-Leach-Bliley, the Financial Services Act of 1999, gave banks, financial institutions, their affiliates and their non-affiliates, that sounds like the universe to me, the opportunity to use and share medical records.

Now, there's an FDIC notice on medical privacy that says that they may not, may not use your medical records to make credit determinations. Okay, great. But they're going to share this information within the financial system the same way that they share credit reports.

Now I don't know about you but if they're looking at a folder and here's a medical record and here isn't, how do we know what they use to make a credit decision if they have that information? Patient Privacy Rights has worked really hard to make the distinction between privacy, which is the right of control, and security issues. And so outside that sort of barbed wire fence, my Texas touch, are the hackers and the cyber thieves and we've amended this slide. Some of you may have seen it before. We've also put the patient and the doctor and the family outside. Those are the people who can't get electronic information either.

Okay. Alan Westin recently did a very detailed survey because the Institute of Medicine is studying the effect of HIPAA on privacy and on research. And he found that only one percent of Americans would agree to the unfettered access to their health information for research. One percent, that's it. The other part of his studies showed that Americans are very supportive of research. And by research I mean it more broadly than the ways it's trying to be sliced and diced, quality improvement, patient safety, those kinds of measures. In the public's eye, all those kind of things are research. People want to support research but they want to be asked and they want to give consent.

That top figure, 35 percent of Fortune 500 companies admit to using medical records for hiring and promotion. It is in the HIPAA privacy rule. Some of you may remember the Walmart famous Chambers memo where there were recommendations made that employees job descriptions be changed and the benefits be changed based on their health conditions and the health conditions of their spouses and the costs.

So the point is that employers use this information identifiably. And that's why I founded Patient Privacy Rights. Employers should not have access to health information. They should not. You shouldn't have to choose between a job and your privacy. If you really think that the public doesn't want to have informed consent then let's go ahead and have audit trails of where and how far health information is going today.

This is one example that I want to show you from a large analytics data miner and data aggregator. This is from their website; a white paper that I can send you because it's not on their website any more for obvious reasons. These are the datasets that are supposedly de-identified that they sell to major employers and whoever else wants to buy them. If you know anything about technology you'll recognize that there's way too much information in here for this to possibly be de-identified.

And that's another problem. You really have to understand in this world that no matter if you take out all the 17 identifiers in HIPAA to qualify for HIPAA de-identification, it still can be re-identified because longitudinal health records have too many specific places and dates that cannot be scrubbed. The data cannot be scrubbed. So de-identification is not enough in today's environment. We have to have penalties for re-identification and for use without consent.

This is something I'd really like you to think about. This is from the same aggregator. Look at what the data is that they're selling and who it's from. I ask you, how did they get Medicare data? How did they get Medicaid data? How did they get this information on the uninsured? The point of this is for you to really think about how far information goes that we and our coalition are doing everything to help the public understand about, because this is the reality today. Health information is primarily used for purposes that have nothing to do with helping you be better.

Every prescription in the United States is for sale, has been for sale identifiably for over a decade. I'd like you to read that chilling language by the inventor of Next To, [misspelled?] the U.S.'s largest stealth data mining system for prescriptions, that's now owned by I think it's United Health.

So we've started a campaign this year for prescription privacy because we really believe that the public will be appalled when they understand that their prescription records have been sold. And by the way, we are not for e-Prescribing unless we fix the theft of prescription records.

And are there solutions? Absolutely. We think that the consensus is to use smart technology that protects privacy backed up by smart legislation and smart certification. What kind of technology? Well, there's smart technology like the Independent Health Record Trust Act. Americans should have one kind of place where they can collect and keep their data that only they control and that is not data-mineable. That is the first thing. It would be like a system of financial banks, but the fiduciary duty is only to the patient.

Secondly, we need independent consent management tools. It's not going to be possible to set consents in 50 places. We've got to have one place where we can do it quickly, electronically, at the granular level. If you prefer, if we prefer, but with directives, blanket directives if we want like what kind of information do I want out about me in an emergency room or that I want my internist to have everything but my podiatrist to have only my medications. You could set and control these and change these instantly and have audit trails.

And the last thing that we've decided to do in this environment, because many technology vendors have begged us to do this, is to start certification by a trusted group of consumer organizations. So we are launching Privacy Rights Certified and we're certifying within the next 30 to 60 days Microsoft's Health Vault and also a company that puts electronic medical records in 2,000 physician's offices called E-MDs because the other certification systems are foxes designing the hen coop and we're sorry, as consumers we chickens don't like that. Thank you very much.

ED HOWARD, J.D.: I don't think I've ever heard anyone describe you as a chicken, Deborah. [Laughter] Similarly, I guess, that would be an attribute I never would have heard John Rother described as. He is in fact our last speaker from AARP, representing the Divided We Fail coalition. He's well-known to

---

most of you, I bet, having lent his thoughtful voice on a range of issues affecting older and younger Americans over the years. He used to labor at the Center of Aging Committee office just on the other side of this wall many years ago, so he knows his way around the hill as well. And we're pleased to have him frequently on our panels. Welcome back, John.

JOHN ROTHER: Thank you, Ed, and I want to thank both Jodi and Deborah for a constructive tone here, because I do think that it's time to break the gridlock. And I do think that we can come together to agree on a path forward. But there are some differences; I'm going to point to those, but certainly the time has come to make a forward move on this because the gridlock has stalled us on some very important advances in health care in the last few years.

So I'm going to just quickly repeat some of the same things that have already been said by Jodi and Deborah, which is the goal here is to make health care safer, better, less expensive. And we need information technology to accomplish those goals. Instead what we've had is very uneven progress and very fragmented situation and many health providers understandably are reluctant to invest in information technology without understanding, without an agreement on what the standards are. So we certainly think that we can work together. This is the year to move it forward.

We also think that we have to have consumer confidence. I think everyone's made that point. Trust is the bedrock for a sound record of health information that contains your own personal records. And for that to happen we have to have rules that consumers can trust, but we also have to have rules that address the inefficiency, the quality problems, access problems in health care. I mean, what good does it do to protect people's privacy if they can't get the health care they need? Also need to note that the current system has, as Deborah's also pointed out, is riddled with confidentiality and privacy problems. And paper records, believe me, are no guarantee of privacy.

So just the fact that we're talking about electronic records does not by any stretch of the imagination mean that we're exposing people to more risk. In fact I would argue that your records, your information can be more secure under electronic systems than with paper. And so I was also happy to see Deb make the point that it's a false choice between privacy and health IT; that we have to reject that. The only way forward is to figure out how best to reconcile the two.

I'll just briefly mention the history, and it goes back a ways. This issue has been before the Congress ever since 1979 and it's been a history of difficulty in addressing it legislatively. HIPAA was debated and no agreement was possible

---

legislatively so it then went to HHS and we've had a more recent failure to conference the HIT bills. This is a very complicated issue. It's very hard to work everything out in legislation. And so today we probably need to go beyond HIPAA, but if we try to sit down as a Congress and work through all the details, all the very complex situations, I think we're going to be here for a very long time.

I would also second the point that Deb made about public concern. Certainly we do believe many consumers are concerned about their health care privacy. I think with some reason. And certainly the headlines about stolen laptops and that kind of thing are feeding the concern, although I do not thing that's the major problem we should be worried about.

So let me just go then to some of the points that Jodi made. The potential is to make health care safer and less expensive, better for everyone, huge potential. HIT can provide comprehensive access to comprehensive medical records in a way that's practically impossible without it. It can engage consumers in managing their own health in a way that's impossible without it. It can allow caregivers and providers to coordinate care in a way that's impossible without it.

And today conditions that are chronic, people with chronic conditions, account for at least 75 percent of the health care dollar. That's the driver for some of the problems we face in Medicare, Medicaid and health care generally. We're not going to be able to really attack those problems effectively unless we give people, the patients, their caregivers and providers the tools to better manage that care. And of course we know that some care is more effective than others and HIT can help us identify, comparative effectiveness can help us identify which interventions work best so that we can better manage our health care dollar. These are really important things and I think that they're not something that we should sacrifice lightly in the name of too strict privacy protections.

So I think I've made this point. I'll just be really quick again. It's easier to track information electronically than it is on paper. It's easier to have an audit trail. The patients gain the ability under health information technology to review and comment on records that they otherwise rarely see. And most importantly it's possible to control who sees that information, which is not possible under today's paper system. And of course we know that there are certain categories of information that are particularly sensitive, mental health, HIV, reproductive health, just examples of that. And so under HIT it is possible to have a particularly tight control over that aspect of your health record and that's also not so possible with paper records.

Just a few other points about how a framework for privacy, an agreed upon framework can improve health care and improve privacy at the same time. We have to address a potential for breaches. Data mining, misuse of sensitive personal data, all those things that Deborah pointed to, will undermine consumer confidence that is vital to the success of this effort. So they have to be addressed. There's no alternative there. And we also have to make sure that people see these protections as adequate, as protecting them from the possibility of discrimination or embarrassment because we don't want people to withhold information or forego treatment which is what happens today. Finally, again, it's not only consumer confidence it's medical ethics that are at stake here as well.

So how do we go about balancing? I would say it is a question of balance. I think that consumers want the benefits and the convenience of electronic records even though they are concerned about misuse. We understand that aggregated and de-identified data have enormous power to identify public health threats, influenza, the spread of communicable diseases, and also most effective care, best practices. This is a really powerful tool to get a hold of our health care budget. And we also saw though, that overly stringent privacy rules can very definitely inhibit research and inhibit the potential gains from better understanding our health care.

Okay. So let me close by saying that we do have some legislation in front of us, namely the Wired for Health Care Quality Act, which has unanimously passed the Health Committee sponsored by Senators Kennedy, Enzi, Clinton and Gregg, which sets up a process where the stakeholders do come together to work on privacy rules, but because those rules would not be fully embodied in the legislation that's what's controversial. So they instead set up a regulatory process to address all the detail. So we have the potential for gridlock here over whether explicit rules need to be in the legislation or whether we have a framework in legislation that can be delegated to a regulatory body. The House is also considering this soon. I think the House would prefer for the Senate to go first and certainly the Senate is the key point of decision for this.

I would say today we embody kind of the three major positions on this. I think Deb would probably say Congress must enact strong protections in legislation. I think Jodi's thrust is that we should let the market play out and let 1,000 flowers bloom and see what emerges out of that. And certainly my position is that we need to break the gridlock now to take advantage of this. And we need then the framework in legislation, but a regulatory approach as a pragmatic way forward. We're part of something called the Consumer

---

Partnership for eHealth and we believe that balancing privacy and the health benefits are critical to resolving this today.

So finally I just say that we do support very strongly the Wired for Health Care Quality Act. We hope this moves forward. It certainly can be improved, but it's critical that this move and break the gridlock if we're going to improve our health care system. Thank you.

ED HOWARD, J.D.: Thank you, John. The Wired for Health Care Act is one of the ones detailed in that side-by-side in your materials. I believe it's on blue paper if you have trouble finding it. There are several other bills listed there as well.

Now is your chance to ask questions, offer comments. There are microphones that you can see that you can go to and ask your question orally. There are green question cards in your materials if you want to write it out and hold it up. Someone will bring it forward. Let me take advantage of some questions that have been submitted in advance while we're getting started here.

And I guess I should admit that this one was submitted in advance by me. [Laughter] I'm sort of in a unique position to have recalled this, and that is that it was several years ago now that Newt Gingrich was one of our panelists on an HIT-oriented program. And what he said about this issue, although not addressing it directly, was that we ought to learn from the experience of the banking industry and the use of ATMs. Let people opt in. If they don't want to use it fine. If we make it so clearly valuable that virtually everybody would opt in, as most of us have in the case of ATMs, the system can function well enough. Now, I wonder, our panelists might think that is a reasonable way to pursue this issue or not? I'd be interested in your reactions. Deborah?

DEBORAH PEEL, M.D.: Sure. We, consumers, absolutely believe in opt-in and if the product is valuable and useful and protects privacy we'll certainly support it and participate. I just wanted to tell you I'm not paranoid even though I'm a psychiatrist, but you did not get to see the over 50 organizations from across the political spectrum that lined up to support strong privacy protections in the health IT legislation. And they include things like AIDS Action and the Gun Owners of America, Microsoft Corporation and the Family Research Council, Cyber Privacy Project and the Republican Liberty Caucus.

Anyway, I hope you'll go on our website and look at this. Yes. I mean, it's fascinating to me as a physician. Everyone is trying to impose health IT on consumers and physicians and everyone's balking. Well I guess we're balking because there are many concerns. Privacy is key. Usefulness of this system to patients really has to be shown in a practical kind of way.

And in terms of market forces I really like the ATM analogy because one of the things that ATMs do is they manage the different legal and regulatory systems for— in every state in the nation so that you can get your money wherever you want it. And the privacy laws in all 50 states are not a block to exchanging information by any means, and that is what technology is really good at dealing with is systems where there are many variables.

And so I think that that is a really sort of apt analogy and we're also again, the decision by Microsoft to stand with consumers last year was a very powerful signal to the industry that privacy is the business model of the future. And that's what we're saying. Ten years ago would every corporation have had to be green? No. Today they are. Privacy really is the future and the technologies that offer us the most control while the information gets to where we want to get when we need it to be there, is the wave of the future.

ED HOWARD, J.D.: Thank you. Jodi?

JODI DANIEL, M.D., M.P.H.: Sure. We have been discussing issues of opt in and opt out. We have a recommendation from one of our advisory committees that we should be looking at this issue. We are working with the

American Health Information Community, the Confidentiality, Privacy and Security workgroup, who are debating this issue currently to try to figure out what the right answers are. What I would like to say is from HHS's perspective and from my perspective, we don't have the answers. We are looking to try to engage the stakeholders in this debate.

So I can't say that this is the right answer. We're looking at the roles of consumers and having greater consumer involvement in these decisions and as part of the protection regarding privacy and health IT. So I would say that from our perspective we're open to that as a possible approach. There are many health information exchange organizations that have either implemented an opt in or an opt out approach successfully. And so we're looking at that experience and trying to learn from that experience.

The one other point that I just want to make as far as when John had made the comment about my position, or HHS's position, I don't think that's accurate. I think that we're looking at all of the different options and keeping all the options on the table. I would say there is some concern about putting things in statute that make it difficult to change over time. John had mentioned that there's been some gridlock on some of these issues when they do come to Congress. And so that raises some questions in our mind and some concerns, but we're working with folks on some of those legislative proposals. We're looking at what authorities we currently have in regulation. And where we don't have authority to regulate we're looking at how we can make sure there are appropriate protections through other mechanisms.

ED HOWARD, J.D.: John?

JOHN ROTHER: As high as my admiration for the former speaker is, let me point out some differences between getting your cash out of an ATM and allowing information to be used by professionals to help you better manage your own health care and stay healthy.

Number one your ATM is not involved in life or death decisions. You may be wheeled into an emergency room unconscious and people who are trying to save your life need access to your health information in that situation.

Number two, health care is at bottom a community enterprise. Communicable diseases are just one example where it's important for people to be able to track that and to be able to take measures to counteract that. That's not true with money.

Number three, we as representatives of the people are managers of a huge health care budget. We are faced with a huge challenge which we're not faced with in banking of trying to make better use of those dollars. This is information that

---

is not only important to the individual to make better use of his or her own personal resources, it's also ultimately important in terms of managing the system.

So I could go on, but there's lots of differences. I do think that we can't resolve this on an oversimplified basis. It's not just about opt in, opt out. It's much more complicated. And that's why, I think, giving this to a sophisticated group of people who are really going to work at this is the most likely way to produce a workable system that does protect privacy. Simply saying it should always be opt-in is not going to get us there.

ED HOWARD, J.D.: If I can just expand on something that you said, John, in your remarks to make sure that people understand it. Those of you who didn't live through it might not be as familiar with it. Congress passed HIPAA, which had privacy implications, and said, "If we don’t' act in the next three years to give you some more guidance then we want HHS to act." They didn't. HHS was required to, which goes to your point about how tough this stuff really is. And which seems to fit your current recommendations.

We have a number of questions on cards that actually I think are quite useful in explicating some of the aspects of this issue. And we're going to start with a reference back to HIPAA. How does experience with the standardized billing under

HIPAA, which was done under the label of administrative simplification, inform the perils and possibilities of larger HIT efforts? Jodi? You've been nominated.

JODI DANIEL, M.D., M.P.H.: I think this goes to the point I think that I was making about the dangers of putting something in regulation or statute that is very difficult to change. I think that HIPAA provides some very important protections. I came onboard at HHS in helping draft the HIPAA privacy rule, so I do think it is important to have those strong protections in place. But with the standards, the HIPAA transaction standards, the process requires a standard setting body to identify appropriate standards and then requires HHS to go through a rule making process, which takes about two years to go through through comment and notice rule making in order to get those standards incorporated into the law.

So what happens is we have standards that all of the industry wants to use to improve the efficiency of those transactions and it takes us three or four years to actually put them into the regulations and make them law and adapt from the old position. I think it is an interesting lesson that we should learn from. I think that it's important to have protections in law. And we do have protections in law, but it's also important to look at how we can layer on top of that with our other mechanisms that we have, providing guidance of best practices, using our contracting methods, working with the states that do have additional protections to help them think through how those protections in an electronic health exchange environment.

ED HOWARD, J.D.: Deborah?

DEBORAH PEEL, M.D.: Yes, I'd just like to point out that the part that consumers want in statue and that Congress years ago couldn't put into statute was a right to health information privacy. That's pretty simple. And the regulatory process eliminated those rights that Congress intended for us to have.

So, we think it's absolutely essential that Congress set that standard. And the Trust Act, which is listed in your form here, really embodies all of the kinds of privacy protections that it's going to take for the public to trust the system. And we feel that really the idea that stakeholders can participate in these national bodies and make up the rules instead of law makers who we can unelect if we're not happy with their decision, there's quite a difference there; these unelected, industry-appointed, bureaucratic decisions that are made, really essentially without much consumer input at all is not going to cut it. Consumers really do have an interest in the laws that come out of Congress and electing Representatives and Senators that reflect their positions. And our position as

---

consumers has actually been uniform across all 50 states. All 50 states have very strong laws that require consent in most circumstances. There is a national consensus on privacy and it's in every state and has existed for 200 years. And we're not going to be satisfied unless Congress restores our right because we don't trust the agency to do what's in our best interest. The track record has not been good.

ED HOWARD, J.D.: Jodi?

JODI DANIEL, M.D., M.P.H.: Thank you. I would like to say, I agree with Deborah on the point that consumer input into the discussions is critical, and that we need to make sure we're reflecting the interests of consumers. On the privacy rules, the first privacy rule, when it came out in 2000, there were 52,000 comments, about 40,000 plus of those were from consumers.

I read a lot of those comments as did every single one of those comments were read, reviewed, considered, addressed in the rules. And when people talk about the length of those privacy rules that's because we were responding to 52,000 comments and we have an obligation to explain how we reacted to those comments. The regulation text is a lot shorter than the 1,000 pages. But I think that the notice and comment rule making process that we did through for the existing rules did

---

require that we got input from consumers as well as other stakeholders and we did incorporate those.

I would also posit that the HIPAA privacy rules took a huge step forward with respect to patient's rights. Before the HIPAA privacy rules were in place there was no nationwide requirement that patients can have access to their own records. That's a huge right that was put into the privacy rules that did significantly advance patients' ability to see their information, to understand their information, to control their information. And in fact if we look at the complaints that we get it's one of the most common complaints we get are when providers don't grant those rights and HHS has been able to go in and make sure that the patients do get access to their information when it's requested.

So I think there are folks who may say that the rules didn't go far enough, that the changes in the rules were not what they wanted, but the HIPAA privacy rules, from my perspective, did in fact advance the discussion and make every health care provider think about these issues beyond the way they had thought about them before because there was this regulatory scheme in place.

JOHN ROTHER: Yes, if I could just say—

ED HOWARD, J.D.: Yes, John.

JOHN ROTHER: I mean, I'm sympathetic of course as a consumer to say that rights should be enumerated and there should be enforcement and we should have very detailed rules. But the practical effect of that position, I think, is further delay and further gridlock. And it's not serving the cause of improving the health care system, making it safer or saving money or really advancing the broader interests that consumers have.

So, while I'm very sympathetic to the points about as much as possible should be in statute, I think as a practical matter if we're going to get going on improving our health care system we have to do it with legislation that establishes a broader framework that sets forth principles. And that does delegate, as is typical, the details to the regulatory process. And so I think that the key point here is that we have to come together. Maybe everybody has to give a little bit if we're going to move this forward.

ED HOWARD, J.D.: Let me just— there's a question that actually gives you a chance to talk a little more about possible areas of compromise. And it reads, "Could someone discuss what other countries and for that matter the VA in our country have done regarding HIT and privacy and how your concerns or desires overlap or differ from those approaches?" Do we have some lessons to learn, Deborah?

DEBORAH PEEL, M.D.: I'm not an expert on international law, but certainly in Europe data can't be collected without affirmative opt-in and the standards for privacy are really quite different. In fact you might know that Europe is considering making IP addresses personal information that can't be collected. They're debating whether an IP address you ought to have control over and we can't seem to get clear in Congress that patients have a right to health information privacy. We're not in favor of having Congress map out all the details of how a right to information privacy would work, but we're not going to trust a system where we don't have a federal right to health information privacy. There was another part to that besides the international question?

ED HOWARD, J.D.: The VA.

DEBORAH PEEL, M.D.: Oh, the VA. The VA system is—we've had whistle blowers write in about it. There's no role base to access, virtually anyone whose part of the VA system can see any records. We got one dramatic letter from a whistle blower who wrote in and said that a patient was getting a shoulder X-ray and the X-ray tech asked him if he was still suicidal. So he stormed out. That's the kind of systems that we have in place now. That kind of thing could not easily happen in a paper system.

And I agree with you John, the technology can give us exquisite control over who sees which parts of our records. It can give us audit trails. It can give us easy access to the information like you're talking about, Jodi, but none of this is going to happen unless people really understand that the system is trustworthy. And the only people they're going to trust is themselves.

I've just got to talk about this as a mental health professional. You probably know this, but 30 to 40 percent of people with mental illnesses are off the grid. No records anywhere because they've been harmed. They see people like me. They pay for care out-of-pocket. They go to AA. There's no information.

So I am very, very concerned if we don’t build a system where people with mental illnesses trust it, we won't get enough data to know what effective care is. I really want quality care. I mean, I'd love to have the ability to study a million people who have been on anti-depressants over 10 years to see which one to choose next. We'll never get the data unless people trust the system.

JOHN ROTHER: Just on the point of international experience, I think that we have a lot to learn from other countries that have developed not only health care that covers everyone, but health information that covers everyone. And most of the European countries are far ahead of us on this, and they do have privacy protections. And the issue doesn't seem to be as difficult in Europe perhaps because most people feel satisfied that in fact that information is protected. So I know there's continuing debate to even tighten it further, but I think we have a lot to learn from some of our colleagues in other countries about how to do this right.

JODI DANIEL, M.D., M.P.H.: Just to add one point on the international discussion, again, I also am not an expert on international law or international policies, but there is, I think, and interesting place that we should look.

In Canada they have a very interesting process to look at their health information technology activities as well as the policies related to those activities. And then did have a very comprehensive process where they were bringing together a lot of stakeholders to work through these issues. They have included in their approach many protections of the data from asking information, for giving patients control of how that information is flowing, and they actually might be a good place to look to perhaps learn on what they've done, how they've done it and where they ended up.

ED HOWARD, J.D.: Very good, thank you. This next question is sort of in the news you can use category. What does it mean, if anything, when you're required to sign a form

---

in your doctor's office saying you have been advised of your HIPAA privacy policies or whatever it says? Sure.

DEBORAH PEEL, M.D.: Well, yes, that's a fascinating piece of this whole discussion. Everyone thinks because they get a privacy notice they've got privacy. But if you read it carefully it actually tells you exactly the opposite. We study the privacy notices from all across the country. They are supposed to tell you what are the stronger privacy laws in your state and how do you exercise rights at the state level. And we never found one that instructed patients how to exercise their rights due to the strong laws at the state level. It simply sets out most of these, virtually all of these privacy notices we've seen simply tell you what's allowed because of HIPAA, which is rampant data sharing and use by entities that you have no control over.

And so it's very confusing. It's very confusing to the public. They think it's a consent form. You probably know this, some offices even say you have sign this or we won't treat you. That happens to be illegal according to HIPAA, but there's tremendous misunderstanding about these notices and they're intended to tell you what the office or the hospital is going to do with your information. And you're just acknowledging, if you sign it, that they've told you what they can do with your information. And some of them will say things

---

like it may be shared with credit bureaus and so forth. We have examples like that.

JODI DANIEL, M.D., M.P.H.: I would just like to say that the point of the notices is based on the fair information practice principle which has been around for a few decades; that you should have openness and transparency about how information will be used and disclosed and what the policies are. The notice is designed to do that, to tell people how their information can be used and disclosed and that they can make decision either to not provide information if they choose not to once they know how it is, to know how they can get access to their records to know what rights they may have with respect to the information that the health care provider is collection about them.

So, it's really trying to implement the concept and the principle, which I think is a very important principle, that patients have a right to notice and transparency about how their health information will be used and disclosed and what rights they have with respect to the information that others are holding about them.

ED HOWARD, J.D.: This one is initially, anyway, directed to Deborah Peel. You seem to suggest the questioner writes, that policy makers or the public and press shouldn't have access as presented in the slide, Medicare and Medicaid

---

Data For Sale. These data are publicly available, and although based on individual claims they are not individually identifiable. How would policy makers be able to make informed decisions without access to these data?

DEBORAH PEEL, M.D.: Thank you. AS I tried to talk about first of all there really is a problem with the de-identification of data and the use of data. We are very concerned that these data, and that's the reason I showed you that particular slide, can be easily re-identified and those datasets are purchased by large employers, and so it's very easy to re-identify data.

So, that's a problem that I don't think we all anticipated years ago when we started thinking about using this information for research because we all want research. But when we know that de-identification is not enough to protect data then we believe that consumers should know about that risk and should have the opportunity to decide to participate in it. And that's a standard, by the way, of research ethics, that they're supposed to get consent before participation.

One of the things that electronic records could do and electronic consent could do, is it could relieve the tremendous burden that used to be on researchers to get consent. I mean, if you think about paper-based systems the reason that we've got IRBs and privacy boards is because if you wanted as a researcher to search across thousands of people or even potentially millions of people it could be extremely costly and time consuming. We have technology now that can make that extremely easy. It can remove the administrative burden and include people and inform them in research. The consumers really want to be part of research, but they deserve to know the risks and who's doing the research and if the project is really something that they approve of.

Or they could even be paid to participate in research. I mean there's nothing that says if we had a health banking system that researchers couldn't pay or even the ones that do prescription data mining couldn't pay you to get your data or your prescription in a de-identified form and aggregate it that way. I mean why should IMS Health make two billion in 2006 selling prescription records when wouldn't it be nice if our parents or our grandparents could get paid for some of this research? Maybe they could afford some of the medicine in the first place?

So, if someone's going to monetize health information it ought to at least be the consumer that does that. But again, research on, and the idea that the data is owned by the government because the government pays, I think most of us would object to that characterization. We pay for our health plans. We pay for taxes to take care of people that aren't covered. And those of us who pay for care privately are also subsidizing the Medicare and the Medicaid and the cost of treating the uninsured, we think it's the individuals that really own the data not the payers. We really think that individuals are doing this. And absolutely I pay taxes and I don't want to pay excessive taxes to cover Medicare and Medicaid, but the point really is we need to give people the chance to consent to the use of their data, particularly when these systems have abysmal security, when many of the systems that hold the data by contract own it and can share it.

So, we have to address all of this so that security is really a big problem, but most of the vendors for PHRs and EHRs for example, the business model, is selling your data. This is just not acceptable. We've got to make this a system that really works for patients and we can get all the benefits by using consent and getting buy in out of respect and autonomy for people's rights.

JOHN ROTHER: And just to say, I think that the example of Microsoft and soon Google, in terms of making available personal health records that cannot be sold, cannot be shared without your consent is a laudable one, and it's helping us to move this forward. But I do think Deborah, that your basing a lot of your comments on distrust. And I don't think we're going to get there if that's the attitude. I think that the point here is to try to build a system that earns the trust of consumers.

So while we have obstacles, while we're certainly not there now, I hope we can focus more on how to get there rather than on stoking people's fears of misuse, which is certainly possible today but hopefully would not be possible under the kind of system we want to build.

ED HOWARD, J.D.: Here's a question that has been touched on in several aspects by all of our speakers in the course of discussion. It simply stated, "Are consumers adequately represented in the regulatory process when considering IT privacy standards." John has laid out a proposal, if you will, that would delegate a lot of the detail writing to a regulatory process. Jodi has talked about spending three or four years trying to get to a decent set of regulation. And in your materials there's a piece of testimony by Sam Carp [misspelled?] from the California Health Care Foundation before an ION panel in which he says that while the current data standards development is promoted as inclusive, in practice the intensive and ongoing time requirements limits active participation to large IT vendors and other large institutions. If that's the way we go how do we make sure that this result isn't what comes out at the other end?

JODI DANIEL, M.D., M.P.H.: I'll start. I think that those are absolutely legitimate concerns and I think it is a continual challenge to try to get consumers engaged in these discussions. I agree that it's absolutely important and I also agree that it's a huge challenge and obstacle that we're trying to address. With respect to the regulatory process, I did mention that we did receive tens of thousands of comments from consumers. That isn't necessarily an ongoing participation and discussion, but it did, there were enough organizations that reached out to consumers and got them involved in the debate and in the discussion.

With other projects we're doing, I mentioned the Health Information Security and Privacy collaboration, we've required that all of the states involved in that involve consumers in their discussions and in their process. We've had representatives from consumer groups speak with the folks that are managing that project in each of the states to talk to them about how they can better engage consumers, how to reach out to consumers, where to look for consumer organizations, where to look for the consumers themselves that may be able to participate.

So, we are continually trying to engage consumers. It's a very important point that the questioner makes. And I do think that we've made great strides in trying to engage consumers and consumer organizations in the processes we're in. Are we there yet? Are we at a perfect position? Probably not, and it's something we have to continue to work on but it is something that we are trying to work toward. It is a valuable stakeholder viewpoint that we want to include and that we are doing our best to try to include in all of our activities.

ED HOWARD, J.D.: John, your—

JOHN ROTHER: From my point of view one of the best statements is actually in your packets from the Markle Foundation, which is a very nice listing of principles and protections that are needed for consumers to have confidence in health IT. And this is the kind of thing that we can build into legislation, not in all the details, not in every aspect, but to set out a framework that ensures that those protections are being addressed. And then turn it over to the regulatory process to flesh it out. So from my perspective I would start with the kinds of things that are laid out in the Markle Foundation's handout.

DEBORAH PEEL, M.D.: Yes, I would just like to point out, I'm not sure that the consumer privacy principles from our coalition for patient privacy are in your packet. Okay, yes, they are. These are endorsed by organizations representing seven million Americans and Markle's original privacy principles I haven't seen this sheet, did not even include the right to privacy. I don't know. Again, the starting point for consumers really is privacy and the comments that Jodi's talking about, both the 52,000 on the original rule when the Clinton administration put out the proposed rule for consent it had, for privacy they did not propose that we have a right for consent. Eighty percent of those 52,000 comments said put consent back into the rules so they did. And when the Bush administration proposed amending HIPAA they didn't say they were eliminating consent, but still they got 11,000 comments and 80 percent of those said to restore the right to consent. But the agency this time did not pay attention to those consumer comments.

So the consumer input really is a challenge. I think one of the reasons is it's incredibly difficult for most consumer organizations to understand the health care system, to understand the privacy laws, to understand how technology works, and of course to have the time and the money to participate. I'm on the HISVE [misspelled?] panel. There's no reimbursement whatsoever. I mean, I don't even get paid a salary for what I'm doing, but there's not even travel money for consumer representatives to come and attend these kinds of meetings. The system is absolutely being dominated by industry and really the only stakeholders, I mean, think about this for yourself, it's you and your doctors fundamentally what we're talking about is replacing a paper system for medical records. And the point of that is to improve your care. We believe that you and your physicians are the real stakeholders in this system, not industry. And so the system, we believe, the way it's set up is very distorted by essentially giving industry, who have real conflicts of interest on the outcome, stakeholder positions in making decisions.

ED HOWARD, J.D.: Pretty straightforward question here, are extra measures being taken to procure trust from minorities in the United States, many of who trust providers and government even less than non-minorities?

JODI DANIEL, M.D., M.P.H.: This is a good question. We have recently been working with our office of minority health, engaging them in our workgroups that are talking about these issues through the American health information community, and I believe they're actually going to be having recommendations forthcoming based on their recent discussions about health IT and minority engagement.

So we have started down that road, we're working with our own, within the experts in our own department to try to address some of those issues, but its' going to be a continuous challenge to make sure that we're addressing the issues of minorities. We also have our HRSA, Healthcare Resource Services Administration, that is looking at health IT in

---

community health centers which serves many minority communities and trying to look at the issues about health IT and implementing health IT systems in those community health centers. So we are looking at it both on the ground level as well as the policy level for our federal advisory committee.

ED HOWARD, J.D.: Jodi, is it practical to have the kind of travel money or some kind of consumer subsidies to make sure that people who don't have deep pockets can keep up with this process which, as you point out, can go on for a long time?

JODI DANIEL, M.D., M.P.H.: I'm not sure I can comment. We have budgetary constraints as well. I would have to take that question back, thank you.

ED HOWARD, J.D.: We'll post it in the hearing record if it comes in a timely fashion. I encourage you to use the microphones. We have a number of questions on cards and I don't know how far we'll get with them. This is also a very straightforward question, might have an interesting answer. Are there interests or industries that have directly opposed HIT legislation? And if so who are they and why are they opposed? And if you represent such an interest or industry you should take the opportunity to seize the microphone and tell us why and who you are.

DEBORAH PEEL, M.D.: I'm certainly not aware of any, are you all? We're very pro-health IT. We just want to use smart technology.

JOHN ROTHER: Well, I think the question is who would oppose a common set of standards that would protect privacy, and I think there has been an opposition from many of the vendors because everybody's got their own product, their own approach. And there's a lot of competition out there. And if we settle on an approach then some people are going to lose out, so I do think that there are, perhaps understandably, has been opposition to moving forward. But the common good here is so overwhelming I really think that it's time to put those concerns aside and we certainly have, as Jodi outlined, we have a rich database already of a lot of different approaches, a lot of different experience, but it's time to move forward on this because we're not getting the potential benefit by waiting around for this to work itself out without some leadership at the federal level.

ED HOWARD, J.D.: Deborah?

DEBORAH PEEL, M.D.: Well, one way that the federal government and Congress could provide leadership is to have congressional investigations into who's doing all the data mining. I mean you're right, John, the people that are opposing this, the industries that oppose this are the biggest data mining industries. And we really need to know what the landscape is and once we expose all this to light I think the opposition to building a system that does everything all of us want, which is protect patients and be able to get the benefits from health IT, I think we'll have it. And maybe you all can get some investigations going because that's the elephant in the room, is all of these other un-consented, unethical, illegal uses of information that really endanger people's futures. I mean, I started this for my kids. I want them to be able to get a job. It's pretty simple. Get a job.

ED HOWARD, J.D.: By the way, you have a job of filling out those blue evaluation forms as we get toward the end of the Q and A period. So I would appreciate it if you would pull those out and start filling them out while we listen to the very first oral question of the afternoon. Would you identify yourself, please?

PAUL LONDON: I'm not sure I like to be first on this, but I was on the—

ED HOWARD, J.D.: And you are?

MALE SPEAKER: I am Paul London. I was in the Clinton administration and I was in the Commerce Department and I went to a lot of these privacy task force meetings at HHS. And it was sort or a noon meeting where a lot of people slept, but it was—

ED HOWARD, J.D.: Just like here.

PAUL LONDON: But it was terribly, terribly dreary. But I will tell you this, and let me address this to Deborah. It was as though there were 30 privacy advocacy groups in the room. I never— I kept saying who are all of these groups? Who are the people? Who do these groups represent? They weren't there, but it was an incredible avalanche of every kind of request for areas of privacy and I couldn't imagine some of the issues that came up from the mostly people from HHS talking about what the privacy groups wanted. So, I think if your complaint, one of your complaints is that the privacy groups or the consumers weren't represented, that's not right. They were very, very heavily represented.

Now, I set up a question. Since 1991 the Institute of Medicine has recommended that said this is an essential technology. Friends of mine, really old people, go to the doctor. These doctors never coordinate the care. It is the most primitive system. Delaying this longer means that we have an artisanal law as you said, a cottage industry of health care where they use technology that would have been perfectly acceptable in 1920, but it's not acceptable in any other industry now.

So I think, I guess the basic point is, consumers have been very well represented and the delay in this means that we have a health care industry that I think is $600 or $700 billion a year more costly than it ought to be. Thank you.

ED HOWARD, J.D.: Deborah, you want to respond? Is it fair then, and one might infer this from Mr. London's question, that consumers concerned about privacy are the ones who have delayed this since 1991?

DEBORAH PEEL, M.D.: I don't know about since 1991. I think it's really pretty simple for most people. It's a right of consent. They want to have the right to consent and that's pretty basic and it's not complex. And Paul, when I was talking about the regulatory process I wasn't involved with it back then, but today all of the panels, all of the alphabet soup of public private consortia and commissions and communities that are working on this issue are heavily industry-dominated. I don't think there's any question about that today.

And so it's very difficult and expensive for consumers to participate in these complex kinds of activities. So you may well be right, I'm sure you're right about what was going on in 1991, I don't know about that. But I do know that now the process is absolutely industry dominated and we don't view their stake as in any way equivalent to that of individuals who are seeking health care. I mean, first and foremost, when people come in to see me they want help with something. They

---

have a problem and they want help. They want to get treatment. They are not thinking down the road about research. They don't cross my threshold looking for quality, looking for research participation or any of that.

The first good and the only reason people come in is because they want direct help. And so if they don't trust we won't get to the common goods of all of the information and research. And by the way, not having privacy, and let me just argue this the other way for you, not having privacy kills because people avoid treatment, refuse to go in early when they're afraid that it's going to lead to loss of a job or loss of their futures. In fact when we were talking with, at the time Chairman Deal [misspelled?] about this, he told the story about one of his constituents whose friend died of ovarian cancer.

So she went in, got scanned, there was a mass, went back, it was larger, doctor operated, saved her life, and then she asked him, "Why didn't you do the blood test for ovarian cancer?" And the doctor's answer was, "Well, you had a new job, you didn't have insurance coverage yet, your husband was unemployed, and I knew if I ordered the test, just ordered the test it would put all that in jeopardy." I don't think we want doctors and patients having to choose like that. That's very, very wrong. And so that's why I say there's bipartisan support

---

for this for privacy so that the health information is contained in the system and doesn’t jeopardize people's futures or lives. That's what we've got to have. That's what we did have before technology essentially, all of these technology companies starting stealing the data. Stealing the data. Even the transcriptionists in Pakistan, once they get done transcribing, sell the data. I mean this is just the thing that we've got to deal with as we build this system, build it right.

ED HOWARD, J.D.: Thank you, Deborah. This questioner writes as follows, "A recent report from the world privacy forum posits widespread personal health record privacy vulnerabilities. Even Google's pilot personal health record platform has been criticized for lacking stringent security requirements. As the PHR movement grows and consumers have more and more control over their health records, how can their privacy be ensured? What sorts of standards, federal or otherwise, should apply specifically to personal health records?" Is there a different answer to that?

DEBORAH PEEL, M.D.: I don't think so. Our coalition believes that the privacy protections should apply to whoever holds the data. And most of you know that PHRs are essentially designed not to be legal medical records so they get no protections under law. We think the protections ought to extend certainly to personal health records and every type of health record, and one of the things that, as I mentioned earlier, that we're doing is we're building a certifying organization that's consumer-led with no industry, to kind of set the standards we want for security and privacy and to rate these projects. We're going to try to move things forward in the marketplace and see what blooms. We think it will be privacy.

ED HOWARD, J.D.: Could I just comment, Deborah mentioned before that she was satisfied with the privacy standards that Microsoft has put into the Health Vault. I reviewed the Google standards. They are just as tough or tougher than Microsoft. I think this is really positive because there are very strong security arrangements, very strong consumer control now and I think we're learning how to do this right. And so if we can build on those kinds of approaches and codify them so that everyone is held to the same standard, we'll really be moving the ball forward.

JODI DANIEL, M.D., M.P.H.: I would just add, I think that the questioner raises a really important issue. PHRs hold personally-controlled health records, hold enormous promise for consumers. I think all of the panelists would agree with that. And I think that we need to make sure that there are appropriate protections for information that are held through

---

these personally-controlled records. I've actually heard along with the questioner that there are some security questions still open on the Microsoft and, at least Microsoft, I don't know about Google, approaches and we need to make sure that there are not only appropriate policies in place, but that there are appropriate security in place. And I think that's actually an area where we would all agree needs to be looked at more carefully and needs to be addressed.

ED HOWARD, J.D.: It has been pointed out to me that I couldn't see because of the lights, that there is indeed a questioner standing at the microphone near the back of the room.

BILL PUGH: A comment and a question. Bill Pugh and I'm from Senator Snowe's office. What Deborah's saying about confidence and public buy in I think is a real issue. Senator Snowe and I know Senator Stabb [misspelled?] and others have tried to promote health IT adoption and I don't think there's any argument here about wanting to do that. If you look at the public polling n the pantheon of health issues it's surprising. We don't have public buy in. It's not a strongly driven thing by the public.

We know it's important. The problem though is if we don't have confidence, and we're talking about why isn't this a problem in Europe and I think most people in the room know why

---

it isn't. It isn't a problem in Europe because in most cases you have universal coverage. You also have job protections. And I've got to put a spin in here right now, or a plug, we have a genetics protection bill that's still stuck here in the Senate.

So the problem that we have here is protecting use. That information gets out and this is why there is concern. And I understand what Deborah's saying. We don't have protection against use of the information. So if the other thing that you want to do is protect possession.

Just about a year and a half, two years ago, I think it was 66 of the Senator's VISA card accounts were breached. A tape was stolen and when we start talking about a fiscal or financial or an ATM analogy to this it's flawed. You can replace your VISA card. And so the question that I'd like to ask just rhetorically, in light of the fact that we don't have protections for this information, how do you unring the bell? How do you make people whole?

ED HOWARD, J.D.: Good rhetorical question, and I don't see any of our panelists leaping to provide more.

DEBORAH PEEL, M.D.: Well, yes.

ED HOWARD, J.D.: We have a volunteer.

DEBORAH PEEL, M.D.: Okay. Well I would say again we've got to have external certification by some trusted

---

consumer-led entity to say that these systems really work. I mean one difference between Google and Microsoft is that Google isn't stepping up to any type of external process to verify that what they're saying is really true. We think that there has to be proof that these systems are safe and then I think maybe people will trust.

ED HOWARD, J.D.: Okay. That's a pretty good summation of at least one aspect of this problem, and I think we will make it the last word, Deborah.

I want to take this chance to thank the Divided We Fail initiative as we have been told to describe it, to thank you for staying with one of the toughest issues that we have to deal with, but one that has one of the greatest potentials for short-term payoff. So don't give up on it yet. And I ask you to thank our panel along with me, I mean, I will along with you thank the panel for what I think is an incredibly good and civil discussion on a controversial topic. Thanks very much. [Applause]

[END RECORDING]
