

>> Manas Mohapatra: Good morning, everyone. My name is Manas Mohapatra, and to my left is Loretta Garrison, and the two of us will be co-moderating our next panel which focuses on privacy issues related to health information. We recognize that everyone has a viewpoint regarding health information, so we expect that our panelists will engage in a spirited discussion about these very important issues. In this panel, we plan to examine the ways health information has migrated outside the traditional medical provider context and discuss the consequences of that migration, including looking at the benefits and risks that may result from the increased sharing of health information. Before we get started, I'd like to briefly introduce our esteemed group of panelists. Starting from all the way to my right, we have Marc Boutin, who is the executive vice president and chief operating officer of the National Health Council. To his left is Kimberly Gray, who is the chief privacy officer for the America's region of IMS Health. Next to her is Deven McGraw, director of the Health Privacy Project at the Center for Democracy and Technology, and to my immediate right is James Heywood. He was the co-founder and chairman of PatientsLikeMe. Beginning with Loretta's left, we have Deborah Peel, who is the founder of Patient Privacy Rights. Next to her hopefully will be Jodi Daniel, who is the director of Office of Policy Planning. She has not yet been able to make it. Next to Jodi will be Linda Avey, who is the founder and president of the Brainstorm Research Foundation. And, finally, all the way left is Stanley Crosley, who is the co-director of the Indiana University Center for Strategic Health Information Provisioning. We are very pleased to have this panel of experts with us today, and before we dig into the substance of this panel, I just want to go over a few logistical items. As with the last panel, audience members can submit questions to this panel by filling out a question card and handing to FTC volunteers who will be circulating within the room. For those people who are watching via webcast, they can send their E-mails by E-mailing them to privacyroundtable@ftc.gov. To our panelists, I remind you that if you'd like to be recognized, just turn your name tent on its end, and we'll recognize you. And we're gonna have to unfortunately keep a close eye on the time, as we have a number of topics to cover with this panel. So, with that I will turn it over to Loretta to get us started.

>> Loretta Garrison: Thank you, Manas, and thank you, panelists, for being here today. We're really looking forward to this conversation. Deven, if we can start with you, what we've traditionally thought of as health information has changed considerably in recent years. With the advent of new technical and commercial enterprises, we have personal health record vendors. We

have genetic testing, medical drug information sites, online health community groups. We have devices that record information and send that information back to the manufacturers. So, what is health information? Who has it when it's no longer limited to just the information between you and your doctor or you and the hospital?

>> Deven McGraw: Thank you very much, Loretta. I'm not sure that the definition of health information has necessarily changed, but the context in which we see it has certainly changed. If you think about where it is defined in the law in HIPAA, it's an extremely broad definition and was purposefully drafted broadly so that nothing would fall out of it, so that essentially all the information within the healthcare system would be considered personal information. But outside the context of the medical system, we might look at it very differently. So, just to give you an example, a heart rate that is taken by your doctor in a doctor's office is medical information. A heart rate that comes from your Nike heart-rate monitor or your Polar heart-rate monitor is still heart-rate information, but we might think differently about it because it's in a completely different context, but it would still fall, quite frankly, under the definition of healthcare information, and whether it rises to the same level of sensitivity or not is a question that's worthy of discussion by the panel.

>> Loretta Garrison: Stan, do these new nontraditional holders of health information raise different sensitivities or suggest different ways in which the information should be treated, as far as privacy or security is concerned?

>> Stanley Crosley: I really, really want to say no, but I know that that's not gonna be acceptable here. No. In fact, they do, clearly, and the problem we have, and Deven already started hitting on it, is that even nontraditional sources are incredibly diverse. So, you're throwing into this nontraditional category everything from insulin pumps, you know, that wirelessly transmit information back to physicians, potentially, to, you know, sites like PatientsLikeMe, right? So, saying that, "Is there a single way to conceive of these things?" is very difficult, but I think it's also very true that health information, no matter where it is, is very different than any other types of information. I mean, there is clearly a societal and an extra you, you know, perspective that you have to consider when you think about health-information use. So, I think you always have to

approach these traditional or nontraditional health-information stores by asking the questions, you know, are they designed to improve the health of an individual or are they designed to improve the health of society or will they improve quality of care? Will they affect privacy? Will they create harm to privacy? And those two things have to be looked at. The juxtaposition of privacy and data control in this context becomes health or even life.

>> Loretta Garrison: Does anyone want to add anything to that? Kim?

>> Kimberly Gray: I think the difference -- Excuse me. I think the different kinds of health information certainly have to be treated differently because they carry with them different risks. Obviously, information that's about a sensitive condition, that particular individual may feel -- should be treated with much more care. For example, the various state laws that now address things like HIV positive status or AIDS or drug or alcohol kinds of conditions, and I do believe that we need to treat health information with some kind of eye towards what the patient's really looking for.

>> Loretta Garrison: Deborah?

>> Deborah Peel: Thank you. Thank you, yeah. Well, I think part of this discussion comes up because it didn't used to be possible for health information to get everywhere. It pretty much stayed in doctors' offices, and now with so many kinds of health websites, so many kinds of offerings on the Internet, health information is not where it used to be and isn't protected, and, so, I don't think we can have exactly what -- I think what someone called context specific protections. Protections for health information have to follow the data or you don't have privacy, and in terms of being able to slice and dice which information in health is sensitive or not, the best person it do to do that is the individual with plenty of information about the risks of what sharing different kinds of information are. So, we're gonna have to develop really robust tools to educate people about the fact that, well, yeah, on your Polar monitor, when you're just looking at your heart rate, that piece of data in and of itself may not be meaningful, but combined with all kinds of other information about you on the Internet and from all the places that collect health information already, it could have very different implications. So, you know, we think that the definition of health information

is broad, as Deven said, for good reason, and people don't understand yet how broadly it's been disseminated, and we believe also that part of the reasons people share health information so freely at health sites is they kind of think that they're like doctors, you know, that health sites are out there to help me with information. They don't understand that many of the websites are business-based models and they use the information which is extremely valuable as a commodity.

>> Loretta Garrison: Thank you, Deborah. That actually brings up a really good point and why we want to have is this discussion about the traditional versus nontraditional context. And, Jodi, can you talk about HIPAA, which everybody knows, but I'm not sure that everybody really understands what it is and what it covers and what it doesn't cover and why that's relevant to this discussion?

>> Jodi Daniel: Sure. Thank you, and sorry for my delay today. First, I just want the disclaimer. I'm with the Office of National Coordinator, not with the Office for Civil Rights. They're the authoritative source on information regarding HIPAA. So, I haven't worked on the HIPAA privacy rules for many years, but this does not represent the department's view. So, HIPAA only protects health information, individual identifiable health information, held by certain entities, traditionally covered entities. These are most healthcare providers, health plans, and healthcare clearing houses which were sort of entities that helped facilitate the transactions between the health plans and the healthcare providers. The new HITECH Act, that was passed last year, did expand some of the provisions to directly hold business associates accountable for those protections. So, what that means is those entities that are doing business on behalf of a covered entity and using individual identifiable health information to do that also have some responsibilities under the HIPAA privacy and security rules to protect information, but what it doesn't cover is a lot of other entities that hold health information, and now that we're in sort of an age where we're trying to help empower consumers, make sure information and data are available to consumers, there are a lot of different organizations that are out there that are holding health information that are not covered by those HIPAA rules. It also doesn't include some traditional entities, like life insurance, disability insurance, and the like that also hold health information. So, it provide as good baseline of protections at a federal level for health information, but it is limited in who -- in what entities have to abide by those protections and what information is protected. So, it's a starting point, but it doesn't necessarily address the gamut of discussion that we're having here.

>> Loretta Garrison: So, the areas that we're talking about that are nontraditional that are not covered by federal regulation that is the HIPAA -- what everybody knows as the HIPAA rules, instead default to the FTC act, section 5, which is fairly broad, very baseline coverage. So, Deven, do these new -- does this context of the new nontraditional holders of health information raise different sensitivities or suggest different ways in which the information should be treated, as far as privacy or security is concerned, and should there be some extension of the baseline that's in the HIPAA world that extends out to certain of this information in the nontraditional world?

>> Deven McGraw: Right. Notwithstanding that we agree that there needs to be baseline protections that follow data wherever it goes, we do not think that the same -- exact same rules should apply for data in the healthcare system as data that's held by commercial entities, specifically because the business models are completely different. Now, I will acknowledge that there's some gray area here where there's sort of mixed healthcare mission and business model approaches out there, but for the most part, for information in the healthcare system, those entities use it to fulfill a mission to care for you, to pay for your care -- whatever those healthcare clearing houses do, which I'm still not sure, but there's a mission that's related to healthcare, and, therefore, the HIPAA rules were specifically designed to allow information to be used for traditional healthcare business operations, caring for patients, paying for care. That's not what Internet companies do, quite frankly. They have a business model to follow, and to some extent, they care that the service that they're offering through their site is seen by consumers as valuable, but their bottom line is to make money or else they wouldn't be putting the site up there. So, to the extent that the risks that consumers face are quite different, you need a targeted regulatory regime in order to meet that, and notwithstanding that the unfair and deceptive trade practices already under the FTC is helpful in this regard. It's not a comprehensive framework of privacy protections based on fair information practices that HIPAA is. So, you know, we can quibble with HIPAA at its margins, but my sense is that it's in general the right approach. We need a sort of similar set of fair information practice rules that govern consumer privacy on the Internet and that would cover health information as it flows there.

>> Loretta Garrison: Jamie, do you have any thoughts to add?

>> James Heywood: Well, I want to go back to your original question where you asked us to define health information, and I think this is the crux of the problem. I mean, it's very straightforward in sort of the existing healthcare infrastructure to define health information as a transaction between a healthcare professional, someone who's paid in a healthcare context, and a patient, and that's a very tight definition, and it works. If you go beyond that, I think we have to actually ask a little bit about what the consequence of the information is and what it means, and health is defined -- at some level could be defined and should be defined -- as broadly as the deviation from normal, whether that is positive or negative. So, for instance, I have my own genome done. I basically have no risks for anything that's detectable. So, if I share that information, I can lower the cost of transactions I engage within the world because I have an advantage, but my sharing that information puts everyone that is unwilling to share that at a disadvantage. So, I'm sharing a positive outcome, or you could look at that in the same way as an intelligence test, which modifies health outcomes, or any variable that is measured, whether that be a heart rate or anything. So, the question about that is, given that any information about someone, their behavior, their status, either at a molecular level or at a behavioral level or at a phenom level, is useful information for someone in a competitive environment, in a bargaining environment, like we talked about earlier. I don't know how you tightly define healthcare information outside of the business transaction process, the healthcare profession itself. You know, and I think what is interesting, and clearly we know an immense amount about our patients at PatientsLikeMe because they share that information as best as we can in a consented, understood environment, but I would argue that Yahoo or Microsoft or Google know far more and could use that information with different levels of restrictions. So, I think we need to look at, you know, fundamentally at what is the consequences of this, and if I could put one more quick frame on this, what I get concerned about when we talk about using health information in a privacy context outside of the healthcare professional world is, you know, we're really starting to talk about the regulation of the flow of information and speech. We're starting to put a restriction on individuals' ability to communicate with each other in the context that they choose in a democratic fashion, with or without, more or less, effectively with content in that process. And we're not talking about the fact that we're supposed to live in a society that was founded on the principal that all are created equal, and we're not talking about the protection of deviation from the quality from discrimination. We're talking

about the inhibition of knowledge about deviation from equality. So, again, we are framing this dialogue not in the consequence of discrimination space, not in the all are created equal under or principal of law space, but that we shall not communicate any deviation from that principle. So, it's a very dangerous space here, because health information is fundamentally anything we know about you that affects your future, and if we define it this way, we're talking about imposing a framework that comes from a historical context that are not really appropriate for human society in dialoguing around this concept of equality and discrimination.

>> Loretta Garrison: Thank you. Linda?

>> Linda Avey: Yeah, I think it's sort of a corollary to that, what Jamie just said, is we should really, I think, spend more time defining the harms that could come from this. I think we talk about privacy, and we don't really spend enough time to think, "What truly could happen if someone got some of your information?" Let's really carry that through to an end point that would be harmful to that individual, and until we do that, I feel like we talk in a vacuum. We got this a lot when I was still at 23andMe, if somebody gets my genetic information. Well, let's parse that a bit. Let's talk about what would happen if someone got your genetic data. You know, could they really hurt you in a very specific way? And when you really dive into that and drive to some points, yes, there are some concerns, and we think this is why GINA was passed. That was kind of the first step to help protect people through their employers or health insurers from discriminating against them. I think there are gonna be a lot of unintended consequences from GINA that we haven't really talked about. One of the things we sat and thought about, like, let's say you interview for a job and the people who interview you just really don't like you and they don't think you're gonna do a good job, so they don't hire you. Could that person come forward and say they found the genes for being an asshole? I'm genetically an asshole, and you discriminated against me for that. I hate to use the language. Excuse my French, but that's exactly the kind of unintended stuff that could happen if we have too many laws in place that prevent the free flow of information. So, defining harms I think is a very important thing that we need to do and spend time on.

>> Loretta Garrison: Well, I agree with you, and we want to do that, but one thing from the consumer perspective is that when they deal with their doctor and they know about HIPAA, what

their understanding is, that there are certain protections, including security protections around the use of that information. What they don't realize is that there are limits to that, and once you step outside the doctor's office, all of those protections, including the security protections and requirements, disappear. Yet, Linda, in your work with 23andMe, you actually imposed those pretty strict regimes around that information in order to provide those protections. That was voluntary. Do you want to talk about why you thought that was important to do there?

>> Linda Avey: Well, in the world of genetics, I think it's a very specific set of issues around genetic data, because if you talk to genetics experts, they will say that if I had about three points in your genome and a little bit of phenotypic information from you, maybe from Google searches, I could identify you very quickly. So, that whole idea of de-identification with genetic data is kind of a myth. So, for that reason, we felt it was very important that we protect the information to the umpteenth degree. You can never get complete privacy, but we do feel like there's so much value in that information, but keeping it in a secure environment and then allowing people to come to you to say, "You know what? If I could, my dream would be to pose this question or this query against the data," allow that to happen and then spit the results out, and in one of our conference calls, I guess, you know, this is very much along the lines of the census, where the information is protected, but you're allowed to go in and do queries of it and get some very meaningful aggregated information back, and that does seem to be a model I think that probably is better in the genetic space.

>> Loretta Garrison: So, if I hear you, what you're suggesting is that there is in fact a place for certain kinds of rules of the road or certain minimal protections in privacy and security around the information. Is that right? I mean, you're not saying that this is just all up for grabs.

>> Linda Avey: Exactly. And I should put it out there that I don't speak for 23andMe, but in my mind, it's important for companies to put out in their privacy policies what they plan to do with the information. And you should read a privacy policy very carefully before you sign up for any type of service that's gonna have your personal information. But on the same token, a lot of companies make the choice that, here's what we're gonna do internally, but then you also should have access to your data, I believe, and if you want that, it should be within your right to do what you want to

do to share it with other people. So, if you have Alzheimer's disease or you have it in your family and you've generated your genetic data, you know what a company's gonna do with it, but you want to take it and share it with other people who are gonna do different things with it. I believe that should be within your rights.

>> Loretta Garrison: Okay. Deb, I know you've been waiting. If you can briefly address it, we want to move to the harms.

>> Deborah Peel: Sure. Sure. What I wanted to say that's foundational to this discussion is the problem with the protections in the HIPAA privacy rule was the key consumer protection was removed in 2002, and this continues not to be widely known or reported, but prior to the amendment to HIPAA, consumers had to be asked for their permission before their information was shared electronically with providers. Today, because the consent provisions were removed, all of the covered entities can make the decisions about using our information, and until we get the audit trails, which were in the HITECH bill, even without our knowledge, and we can't refuse or stop these transactions. So, although I agree with you, Deven, that there are a lot of problems with how health information is used outside of the healthcare system, many of the players inside the healthcare system are using our information and misusing it in ways in ways we would never agree to because we don't control it. For example, all the pharmacies in the United States are data mined, and prescription information is sold daily and used in various ways that the public typically doesn't know about or agree with. So it's important to understand that the key consumer protection was taken out of the privacy rule, and that does make a difference, because many health companies and health IT vendors are using the data and selling it for things that people would not agree to. And the point really is, as Linda says, and really, Jamie, I think as you say, is that people should be able to make choices with personal information. We just believe that everyone should know what the consequences of the choices are and be freely made, and potentially with genetic information, if you make a choice to share it, it could harm other people. So there may be some differences with that compared to other kinds of health information. But people need -- we need entirely new tools that inform people about how the information can be used and how to control it in a way that makes sense to them.

>> Loretta Garrison: Great, thanks. I'd like to turn to the risk issue, and, Marc, if you can lead us off. Are there new security or privacy concerns that are raised with respect to the disclosure of this information and these nontraditional settings? Are there particular risks associated with certain information and lesser risks associated with other or other contexts?

>> Marc Boutin: Thank you. There certainly are risks, but I want to be clear to the earlier discussion. We've been focusing in on risks, but there are also benefits, and I think we need to identify and stratify the risk and identify and stratify the benefit. The National Health Council represents 133 million people with chronic conditions, many of whom have multiple chronic conditions. The reality is they're making tradeoffs in their lives. The technology and information boom has made life very different for many people with chronic conditions. Many people who had death sentences can now live a life with a chronic condition, can live at home, and can use some of this technology to make life better for themselves. I would grant you that there is a complete lack of understanding amongst the general public and certainly amongst people with chronic conditions about the risk here, but many of them are making very calculated tradeoffs to live at home, to live a more independent, normal life with the technology that is available to them. So, clearly we have risks. I think certain risks are more dangerous or potentially more harmful to people than others, but there are a lot of benefits, and we have to look at the risk in the context of the benefit for the individual. And, so, the challenge here is how do you stratify that risk, how do you stratify that benefit, and how do you address what are in reality very extreme viewpoints? When you look at people with chronic conditions, as much as 30% are happy to have their health information used if it's gonna benefit their children or grandchildren in terms of new treatments, but on the other extreme, you have people with chronic conditions who do not want their information used unless they provide consent, and many of whom would say they would not provide consent. The reality is the majority of people with chronic conditions, like the majority of people in the general public, fall somewhere in the middle. So, our challenge is, again, how do you stratify the risk, how do you stratify the benefit, and how do those competing interests weigh?

>> Loretta Garrison: And, Marc, you've mentioned also that when you're a patient with a chronic condition, you're balancing a lot of different things in very different way than the ordinary

individual who does not face those life-threatening or life-impairing problems. Do you want to speak to that?

>> Marc Boutin: Sure. If you look at an issue from the perspective of -- we do this often in Washington, D.C. You look at a young staffer up on Capitol Hill. They may have never taken a prescription in their entire life and their perception here is very concerned about privacy and security. But if you take the context of somebody with Alzheimer's or somebody with a complex autoimmune disease or a neurologic condition, somebody who may be facing death as a result of their condition, their tolerance for risk changes, and they articulate this in this space. Even when you look at the risk of privacy and security breach, which I have to be very clear, they take very seriously, nobody with a chronic condition wants their privacy or security breached. However, they'll tell us in focus-group work and in other studies we have conducted that they liken it to what happened after 9/11. We all face greater security in travel. We all face greater invasions of our privacy as a result of that. If you have a chronic condition and you know that you do not have a viable treatment and you know that your children or grandchildren may face the same fate, you're very concerned about the development of new and better treatments for them. You're very concerned about their lifestyles being better, being able to stay at home longer, having better cognitive skills. And as a result, you're willing to trade off some of that security in that space, and many of these people will say they'll do it without even being asked. So, the challenge is, again, how do you balance these competing interests?

>> Loretta Garrison: Right. And those kinds of tradeoffs would not necessarily be made, as you indicated, by someone who's not facing those life-threatening situations. Deven, can you speak more to this point on the risks, particularly in the context of the merging of health information that's collected in the nontraditional context, merging with online or offline data that's other than health information? Because we're seeing a lot more of that merging of data.

>> Deven McGraw: Yes, we are seeing a lot more of that. I want to start off by responding to some of the earlier remarks. I don't think we have to nor should we go down the road of a Draconian set of rules for consumer privacy on the Internet that essentially cut off the data flow and make people -- and decrease its utility to people for the reasons for which they seek it out on a

regular basis and increasingly so every day. On the other hand, one of the harms that could result of allowing this sort of Wild West environment to proliferate is that we, in fact, decrease people's trust in going there. So, folks who have no qualms at all about having their information shared won't be deterred at all from using the Internet because there's a sort of threshold for privacy and the extent to which they care about it might be quite low, but I'll put on the table that for most people, they actually would like a sort of baseline set of rules, and many of them, in fact, think they're out there and exist when, in fact, they don't, rather than just leaving it to the privacy policy of the company. We actually have on this panel today companies that have done -- that have recognized, in fact, that people do care about this, and so they put in their privacy policy very clear provisions about how that data's gonna be used, but that is absolutely not true for many of the sites that you see out there. And, so, people are sort of in this environment where their data can be sold. You know, if the company says in its privacy policy they won't sell it, then, of course, they can be -- get in some trouble with the FTC if they violate that, but there's nothing that says that they have to make that commitment to people. So, oftentimes, if they even say that, the provisions of the privacy policy become very hard to read, and so we've got this environment where people are putting health information on the Internet probably thinking their privacy is more protected than it is, and at the same time, that data is being merged with a plethora of data that is out there on the Internet about how much you paid for your house, things that you've purchased, and there are Internet-based companies arising all the time that are merging this data together and selling it. We just sat in office yesterday at CDT and pulled up a profile on me where someone was trying to sell a credit report. This was not an official credit-reporting agency, but it was obviously a collection of data points about me on the Internet that had my zip code. It reported that I was married. So, part of that isn't factually true. The other damage here is that, in fact, this information created by data points based on your searches, et cetera, is not, in fact, always all that accurate, but if you're merging that with true health data that people have put up there or that they maybe have put into a personal health record, then you've essentially got again just this incredible database of information that if we don't have protections, basic protections in place about how that's used that are both about how individuals consent in a privacy policy or in a notice of practices but is also about stopping patently unfair or unreasonable behavior.

>> Loretta Garrison: Jodi?

>> Jodi Daniel: Yeah. I agree with a lot of what Deven was saying. I think, from our perspective in promoting health information technology, we're obviously trying to leverage the benefits that you can get from making information available to other providers to improve coordination of care to consumers so that they can better manage their own health and healthcare, et cetera. And I just want to try to tease out some of what we're talking about with privacy and security, 'cause we keep kind of lumping it together. It seems to me that at least folks sort of expect that there are some basic level of security protections that folks can't necessarily -- Even if they want to make their information available to some folks to research purchases or to other consumers, that there's basic security protection so that it's not a free-for-all, that only those who are authorized to get access to the data do. So, there's sort of the security issue in protecting the data, and then there's some of the privacy issues. You know, in the consumer-facing services on the Internet, you know, we talk about privacy policies, and even entities that do try to do a good job of communicating their privacy policies to consumers, we know that many consumers don't read them. Even if they read them, they don't understand them, even if the company's trying to be clear. And there's still a significant disconnect in the understanding of consumers and how information is flowing, what protections there are or aren't, and what they're agreeing to. So, I think there is a lot of room for improvement in the area of transparency and making sure that consumers are making informed choices, if, in fact, they are making choices, or at least know what they're agreeing to when they put their information out there, and, you know, it's very hard to get to a place where you have consumer choice if you don't have that understanding and that transparency. So, I think that is an area where I think a lot of progress could be made.

>> Loretta Garrison: Stan?

>> Stanley Crosley: I agree completely with Jodi. I think that was very well said. The other point I wanted to address was the trust point, because I think trust is absolutely pivotal, in healthcare for sure and nontraditional settings, as well. They think of trust not only as trust on securing the information and the privacy protections, but also think about trust as an outcomes perspective. If people are going a site or gonna a nontraditional using their home healthcare devices, and they're not gonna trust that the information's gonna be used to their advantage or used to benefit their care

or if their quality isn't improved, their quality of life isn't improved by the sharing of that information, then they're also gonna lose trust in the model that they're participating in, right, both the nontraditional as well as the traditional healthcare settings. So, trust has to also be measured not just in -- we have to do everything possible to make sure that the information is tied down, but, also, we have to make sure that the information is utilized to the benefits of the individuals. In some cases, that means sharing the information, and that is really precisely the issue that was faced when HIPAA was first passed, and in 2002, when they took out the consent provision, was so the information could be shared and quality of care could be addressed. So, again, I don't dispute for one second that that decreased the potential of privacy protection. It's hard to argue that it didn't, but I think it also had an order of magnitude improvement in quality of care that came about that. And, so, I think that trust element is really a two-edged sword, as well.

>> Loretta Garrison: Marc, did you have something you wanted to add?

>> Marc Boutin: Quickly, with respect to the benefits. I said earlier there are 133 million people with chronic conditions in the United States. Most of them have multiple chronic conditions. The challenge that many of them have is that when you have a chronic condition, it's usually not visible, and when you think of that number, that's nearly 40% of the population. So, if you count the people around you, 4 out of 10 probably have a chronic condition and you're not aware of it and they're not aware of the other folks with chronic conditions. One of the spaces that this new technology fills is it brings these people together online, and you can't underestimate the value of that to people who feel invisible. People who are sitting in this room can feel invisible. There's important social and health and other benefits in this space. So, again, the value here is to look at those benefits weighed against the risk and figure out a solution that addresses both security and privacy but doesn't undermine the benefits to a point where they're of no use.

>> Loretta Garrison: Deb?

>> Deborah Peel: Yeah. As the only one on the panel that's practicing physician, I think if you all were in my place, and I've been a mental health professional, a psychiatrist, and an analyst for 35 years, you know, you would understand where I'm coming from and why I founded Patient

Privacy Rights, and that is that from the moment I went into practice, people came to me and they said, "If I pay you cash, will you keep my information private?" Why did they say that? Because they had lost a job or their reputation had been damaged because what they said in the doctor's office did not stay in the doctor's office, and so these are very real, very real problems, the lack of privacy, that keep people from getting treatment, and it's not, of course, just job discrimination, but health information is used by insurers, not only health insurers but life insurers, even property and casualty insurers, and banks and financial institutions today are permitted by Gramm-Leach-Bliley to handle and transfer health records in the same way that they share credit reports. So, this information is -- has gone way, way, way beyond the doctor's office. And it's really important I think in this discussion that we don't act like this is an either/or situation where we must share all of our data to get the benefits or, you know, we have to Draconianly not participate at all in the benefits of health technology, and it's a completely false opposition. We should be able to do both to the degrees that we want, and I don't know anyone -- if you were thinking of me, Deb, I don't know who anyone who wants Draconian rules. I think we need to have choices that people make, because there are significant, significant majorities that want and expect these choices because of the harms, and we already know from HHS findings that 600,000 people a year refuse to get early diagnosis and treatment for cancer because they're afraid the information will leak out and affect them. 2 million in my field, mental health, refuse to get early diagnosis and treatment because the information may harm them. You know, and I can say this again, as a psychiatrist, we have to give our patients Miranda warnings almost. Look, if you use a third-party payer or if you get a prescription, this is gonna have consequences for your life, and that's very discouraging to have to say that we shouldn't have a healthcare system where you have to worry about whether you get care is gonna, you know, destroy your future and your life.

>> Loretta Garrison: Thank you very much. We can clearly spend a couple days on this, but we are a little tight on time. So, I'd like to move quickly to a topic about marketing, use of health information for marketing. Kim, marketing or advertising is a major source of revenue for online companies. It's been permitted under HIPAA, although there were additional restraints imposed on medical marketing. Can you talk about the marketing aspects, and, Jodi, if you could also follow?

>> Kimberly Gray: Yeah, I'll be happy to, but I believe, though, that most online marketing does not take place in the HIPAA world. In other words, I think covered entities and business associates are not, for the most part, doing online marketing. I've spent many years at a health plan, and the marketing that was typically done there would have fallen outside of marketing. In fact, it really wasn't marketing, as that's defined under HIPAA. What it really was, was offering goods and services that were health related and were of direct benefit to the patients receiving that information, typically by mail. So, I'm not quite sure how the HIPAA-HITECH world comes into play here. HITECH clearly has made some amendments to HIPAA, as far as its definition of marketing goes, but, again, I'm not really sure where that came from because I don't believe there were a lot of complaints about inappropriate marketing in the traditional healthcare setting. I don't believe that HHS was receiving complaints about marketing being done by covered entities or their business associates, so I'm not real sure what the legislative intent was behind that switch to make the modification under HITECH, but clearly I think online marketing, the use of cookies, targeted markets while surfing the web or whatnot, are not coming from the traditional healthcare world. They are coming from the more nontraditional kinds of things that we're looking at today. I don't know that there is a good remedy for that today, but I'm not so sure there needs to be one. I think studies probably need to be done to see if people actually want to be marketed to through targeted marketing first, and I don't believe that's really adequately taken place at this point of time. I mean, the plus to this is that none of us really want to be bothered by marketing ads that have nothing to do with what we're interested in. Do we welcome those marketing ads that do have something to do with what we're interested in? Perhaps. I don't know, and I don't honestly know. Perhaps others on the panel know if there has been any real research done into this, but I believe that that's probably the first step.

>> Loretta Garrison: Jodi, can you talk briefly about why congress put restraints on marketing within the HIPAA context, and then move to the broader online marketing?

>> Jodi Daniel: Sure. Well, I can't talk to congress' specific intent, but I can talk about what was in the rules and where the challenges are and what has changed in HITECH. HIPAA does generally require an authorization by a patient for use or disclosure of health information for marketing purposes. The challenge is what is marketing. And something -- it's something that is

related to the treatment of the individual marketing. When is something treatment, when is it marketing? So, for example, if a doctor sends out a refill reminder, they're in effect trying to encourage a patient to spend more money on a particular drug, or if there's a new drug that hits the market and they send out information to a patient that might benefit from that new drug, again, one could argue that's marketing, but one could also argue that that is a doctor trying to help provide the best treatment or inform their patient of treatment options. So, there is -- You know, we've had so many discussions on where do you draw the line between treatment and marketing and making sure that you're preventing the -- an entity from doing those things that are marketing that folks are concerned about but not interfering with important treatment communications. So, the privacy rule originally tried to do this and draw this line and say that health-related communications were basically exceptions for marketing, and I'm saying that in a very general sense. What the HITECH Act did was go one step further and limited what healthcare -- health-related communications could be considered a healthcare operation and not require an authorization by saying that if a covered entity received direct or indirect payment for making the communication, then they have to get an authorization from the patient to do that. So, there's still the question of, you know, what's payment, and the office for Civil Rights will come out with modifications to the HIPAA privacy rules or proposed modifications that will address those and ask for comment, but, you know, what the concern was, I think, is that if a doctor is being paid to make a communication, is that somehow different, is the consumer who receives that gonna trust their doctor and not understand that there might be a conflict of interest there because they're getting paid for it? That being said, a doctor in a small practice in a rural community may really feel that it's important to communicate information to a patient but may not -- may be operating on small margins and may not have the resources or want to spend the resources to make those communications given other competing demands. So, there may be some important payment for communications that the Dr. May want to do, and so the question is, again, what is the line of marketing? But I think that there was some concern that if the doctor is being paid to make the communication, even if it's being reimbursed for their costs, that it might taint -- there may be some conflict of interest, and the patient should be aware of that. I think that was the intent.

>> Loretta Garrison: So, Deven, there is some line drawing in HIPAA, but there's no real line drawing outside of HIPAA in the nontraditional world.

>> Deven McGraw: No. Again, you know, we live in this space where we've got a set of rules that apply when information is in the healthcare space and those rules don't apply, and we've actually argued that the same rules should not apply. Again, we've got to have a regime that appreciates the value of the Internet but also deals with the risks, but in the online context, with respect to targeted behavioral advertising -- and CDT has written a fair amount on this -- essentially, there aren't any hard and fast rules, again, beyond what might be in a company's privacy policy, which, of course, they then have to abide by, but they don't have to do one of those in the first place or make any specific promises, and, so, what you see is an increasingly sophisticated attempt to be able to target people with very specific advertising based on their click stream, all of their Internet traffic, essentially, pseudonymized. Not that they know it's Deven McGraw, but they're able to sort of know that it is me, this single person looking at all of these searches. What?

>> James Heywood: And that you're married.

>> Deven McGraw: And that I'm married and that I live in zip code 20004. But there isn't any -- Right now, all that we have to regulate the space is some self-regulatory principles that are not uniformly adopted by all the companies in the space, and we posit that self regulation is not on its own enough to protect consumers in this space, and instead you need some baseline rules for which patients -- Patients. I'm still in the healthcare context. That individuals at a minimum ought to be able to, if it's nonsensitive information, be able to opt out through very clear choices presented to them, and if it is sensitive information, of which we've put health in there, which gets back to our conversation earlier about that pesky broad definition, that people ought to be required to opt in to receiving those ads. So, therefore, you set up a situation where people who want to be targeted, who'd rather not have the barrage of ads that don't have anything to do with them and would prefer to see ads that are much more relevant to their lives and what they apparently care about, based on what they search for on the Internet, can do so, but those of us who don't, don't have to.

>> Manas Mohapatra: Thank you very much. I think we're gonna just shift gears slightly but in a very related sense and talk about consent generally, and I think Deborah already spoke in some ways about the consent in the traditional medical environment based on the 2002 amendments to

HIPAA, but I would like to ask her, what should -- how should consent be addressed both in the traditional medical setting and in the nontraditional medical setting?

>> Deborah Peel: Well, obviously, most people in the traditional medical setting, patients -- certainly my patients and then all of the organizations that have joined our coalition, which represent 10 million Americans, believe that control over personal health information is essential unless otherwise required by narrow statutory limitations, or exceptions. Excuse me. So, we position consent is really the foundation of trust in the systems, and we're not gonna have trusted Internet systems again unless people control personal information. You know, if we look at the broad frameworks that were devised, I think actually first when it was the Department of Health, Education, and Welfare, the code of fair information practices set out general principles for all personal information anticipating not -- I don't think they could have anticipated back then what we have now, but they were beginning to anticipate the problems of ease and dissemination of information and the ability to analyze it that computers brought. So, we really think that we need in this nation something like that. We didn't think there was anything wrong with that scheme, and we need fair information practices for all personal information, particularly because it's very clear -- it's very clear that all this information about us is very valuable, and whose asset is it? Whose asset is it? It should be that individual's asset to control, and what's so important about this discussion is that in healthcare, we have the one area in life and in commerce where individuals have very strong rights and have had them since the founding of the nation. This is the only area where we know, because of Hippocrates, that we really are supposed to be able to control our information, and, so, if we don't protect these rights in healthcare, we're not gonna be able to get them in wider commercial situations. And you all know, I think, that the regimes in Europe are quite different. They have -- even collecting an IP address is considered taking personal information, and there aren't any -- they're not allowed to have secret databases that collect your information. I think we're gonna need to be moving more to fit in with a world where individuals control digital information data about them.

>> Manas Mohapatra: One of the things that's come up in the previous roundtables and has already come up today is about how you get to express informed consent. You may have the fair information principles and you may have a voluminous privacy policy, but do consumers -- do

patients understand what is being done with their information? I'd like to actually direct this to Jamie right now because I know that your company has tried very much to be very open in regards to what you do with the information, and I think, though, you would agree that some percentage, however small, may still not understand what you do with that information. So, how do you get to express informed consent?

>> James Heywood: I think the word transparency, that's sort of in vogue today, is actually the critical element here, which is, can you -- Do you communicate everything as best you can? And I actually think this is important when we think about a new context like the Internet sites like us or the ones that are less transparent. You know, just to think about what we're comparing ourselves to, and I think, you know, when you look at the existing healthcare system, and we've talked a lot about business models and making money and the influence of these things on behavior. I mean, you know, the health system itself makes money. It makes money with mechanisms that are extremely inappropriate and unaligned with patient interests, and there are all kinds of counter incentives, almost bribes in the system, to create bad behavior on the part of healthcare professionals that, in general, resist them, remarkably. And, so, I think in this context of transparency, you really want to say, "Where is your cash flow coming from, what are the components that align to that, what are your goals and intent?" And for us as a company, we've been doing a lot of research on this question, and we actually just did -- we do research on several things. One is, do people understand what we're doing? And the answer is, it varies from 70% to 90%, based on how we ask the questions. There's a dialogue about it on our website. There was a great thread. When someone came in and missed the fact that we have this line on the front page -- "If you're a life sciences company, learn how you can buy our data here." And they said, "You're a for-profit company and you sell the data," and the community responded. There was 121 posts of this thread. There were 21 all positive, you know. "If a life-sciences company wants to buy my data, they care about me." One line said, "If a PhRMA company wants to buy my data, they care about me more than my doctor, because he doesn't want to know." So, I mean, there was this sort of very positive vibe in that in this context for sharing, but then we go and we ask harder questions. We just did a survey, and we asked questions, "Would you share your Social Security number? Would you share your insurance policy? A Social Security number helps us find out if people die, because we don't know when they die, and that's an important variable for us in looking at whether

drugs work or not.” You know, income, race, living situation, relationship status. And we asked the questions two ways. “Would you share this information?” And then we said, “Would you want to find other individuals using this information?” Because they're trying to put that in context. And the numbers came back remarkably high. I mean, 60% or so wanted -- with the exception of income, interestingly. Everything else, they were good with, and income they didn't really want to share. And we're trying to learn what's the right balance, and it's listening to this sort of very democratic open institution that, by the way, when we screw up, they tell us, you know, but I don't think the world operates that way, and you asked a question earlier about rules. “Are there rules and principles?” We don't know them yet. We have a set of values -- patients first, transparency, no surprises -- that we will never meet. There's no way for us to have 60,000, 100,000 people understand. It's not possible. I will say we are, I think by measure, better than anyone else I've ever looked at, but we are probably a long way from what I would define as consent, and I don't know what the rules are. The rules are a set of principles that you iterate towards, and the commitments measure it, and, you know, maybe the willingness to put that data up online, but I don't know how to -- I don't know the answer yet, and we're moving towards that answer. So, I think this consent question is really tricky, and it does come down to trust. It's about -- are these institutions, you know, acting in responsible, trustworthy manners that are aligned? And I don't know how to regulate that.

>> Manas Mohapatra: Marc, do you have some thoughts on this?

>> Marc Boutin: Oh, yes. Thank you. Consent is really, really tricky, and I would agree with some of the comments that consent is intricately linked to trust, and there's clear evidence that there are many people who forego treatment as a result of not trusting that their information is gonna be held confidential, especially for stigmatized diseases and conditions, but consent isn't the magic bullet here, and that's the challenge. Consent, when you look at people with chronic conditions specifically and with the general public, 75% of people don't understand it, don't understand how it work, don't even realize that they have given consent. Now, I'm sitting here and I'm looking at a lot of people. You guys look pretty smart to me. How many people have signed the consent forms when you went into your doctor's office? Raise your hand. Okay. How many of you have actually said, “I'm not gonna sign it” or “I want specific exceptions?” Okay. A couple of hands went up.

That's the most I've ever seen when I've asked that question, and it's because it's very challenging. Most people with chronic conditions are told they're not gonna get care if they don't sign the consent form. The reality is, the current system is not working. I think there are a lot of things that can be done to improve it. There's no question about that, and we should strive to improve it. It is interlocked with trust. But the reality is that people expect our government to protect us in terms of public health, safety. They expect research to be done to improve treatments. We're spending over \$30 billion a year with government money to figure out how to address new treatments. These perceptions are juxtaposed against each other. We want consent to be the key, but yet we want the information to be used for certain purposes. We've got to do both, and I think that's the issue, is consent is in and of itself not the solution, but it's part of the solution, and you've got to look at it in a greater context.

>> Manas Mohapatra: Deborah, we have just a few minutes, but if you want to make a quick point.

>> Deborah Peel: Sure. Well, the problem is for the public. They really do object to having their information used without their permission. Alan Westin did a survey for the Institute of Medicine and found that 1% of the population only would agree to open access to data by researchers. 38% would want to know what the project was about, the purpose, who was doing it, and so forth, whether it would help their family. And another 13% said flat out, even with information, they didn't want digital information about them used. So, you know, this is very important. We don't believe that the entire public knows what public health uses are, knows what quality research is, knows what comparative effectiveness work is, knows what patient safety work is. These are all research to them, and the public -- the public does want to participate. Many people want to participate, and you'll get fuller, better data when they understand that the data's not gonna be forcibly taken from them, and we don't need to do that, and particularly as a psychiatrist, I'm very, very aware of, you know, people's mental state and what they can understand and when they can understand it, and you all are certainly right. There are people that when they're in the throes of illness or they're ill or they have some kind of impairment or they have a guardian, they cannot give consent, but the majority of people, the majority of the middle, really want it and are capable of understanding what's gonna happen to them if it's explained to them, and another benefit of technology is that the technologies independent of when you're sick, we can have robust consent

tools that explain these things at a time when they're not so sensitive and explain the implications of different choices. So we need to have a whole lot better training about consent, and we can make much better consent because of technology.

>> Manas Mohapatra: Linda, do you have...?

>> Linda Avey: Yeah, just a quick comment about this concept of consent. We tend to talk about it, I think, in black and white. Like, you've either consented to something or you haven't, but with technology, I agree, Deborah, that we now have the ability to have a constant dialogue going with people, that we can have them consent and they can change their minds, you know. Some people look at PatientsLikeMe when they're not sick and say, "I would never share my information," and then they get ALS and everything changes. Their life is flipped upside down, and now, suddenly, sharing information could be very valuable to them and their family. So, this notion that we're gonna define this and then everyone's gonna agree to it, that's never going happen either, because we're human beings. We change. Our opinions change, our perspectives change, and one of the things that I think we could focus on is, how could we put language in very simple terms for people to understand as they're going through life and they're changing and they're saying, "You know, I do consent to this now, but by consenting to this, what does that mean?" Can we come up with standard language that people understand and companies can agree to that say, "Here's what you're agreeing to right now at this point and time, with this decision you are making to share this information, whether it's a little language on the top of a survey, but something that really triggers that trust that people say, "Okay, I'm gonna do this, but now I know this is how my information's gonna be used." And if we can come up with that language and that methodology, then I think we're gonna make some headway, but otherwise we can't live in a black and white world.

>> Manas Mohapatra: Well, this issue of consent is an important one and pervades all issues related to health information and privacy and specifically to our next topic, which is about the role of medical data in research, in terms of consent issues related to that. But people understand that there's a big debate right now regarding making medical data more accessible for various critical social needs. Stan, would you like to start us off to highlight some of the major issues in that debate?

>> Stanley Crosley: Sure. And I think one of the major issues is consent. Beyond consent, I think you start with the traditional analysis that you've heard here in a couple of places, and that is, what's the utility to the individual, what's the benefit to the individual, what's the benefit to society? And society really not as a concept that's unknowable but a society of patients who are dependant on discovery of medicines or other treatments. And then, what's the harm? What's the potential harm that can occur with the sharing of that information or with the actions that you want to undertake? And I think it's really important to maintain that framework. One of the issues, and it was raised here earlier, is that, you know, we are on the cusp of -- and just the cusp. I mean, maybe the doorstep of the cusp of really understanding personalized medicine. I mean, we are barely at the place where we are making medicines more safe, right, and we're able now because of either genetic sequencing or finding certain snips and polymorphisms that may identify certain illnesses or certain reactions to certain drugs that we're administering them more safely. Genetic testing. Certainly companion diagnostics can become far more common over the next five years than you've seen so far. So, we are on the cusp of tailoring therapy now, and the first step is to make products more safe. That said, the amount of information that exists in medical records, and even electronic records now. We wouldn't have said that 10 years ago. But electronic medical records, it is staggering. It's why the panel's here worried about the privacy issues, but it's also why the potential benefits are completely unknown. I mean, we can't even conceive of the benefits, and the worst possible step is to say that, "Well, we need to get a handle on medical research and slow it down because we want to make sure that we protect people's privacy." I think we need to make sure we protect against harm. I absolutely believe we need to prosecute harm mercilessly. But I think that the transparency that's been talked about is important. I think consent is very difficult in the medical-records research space. Medical records, as distinguished from interventional research, I think you're gonna talk about that a little bit next. But medical-records research data that already exists that is collected in traditional settings within the healthcare setting. Even a 3.2% opt-out rate, Art Caplan at the University of Penn found, could completely bias the ability of a research effort to conclude a realizable result. Bias because they found that people who opt out have shared issues, and, so, by having those shared issues, you completely bias the research result. That's a safety issue. That's a life issue. People die when information isn't shared appropriately, and that is not a dramatic overstatement. And so it is critically important within research both from a safety

perspective, by a surveillance perspective, and now, as we step into, you know, a pharmacogenetic or genetic research, epidemiological research, and pharmacoepidemiological research, so you'll need to kind of string together genetic information, medical-records information, epidemiology, to understand whether it's an underlying environmental or a genetic or a drug issue. And, so, the only way we're going to advance this medicine is to look at these issues that have been identified on the panel, but I think that with research and within the traditional healthcare setting, there's a far more fundamental issue at hand, and that is consent has an ethic that cuts both ways. If we're saying you have to control your information and know how it's going to be used, and if you say yes or no, then that controls everything else that follows. I think that's too much burden on an individual. We need a paradigm or a structure on accountable use, what is expected for the use and how is that gonna be permissible. By saying, "And if you do that, then this is the frame," and the people who are worried about how their information may be used, you can address the harms that can evolve from that.

>> Manas Mohapatra: Deborah?

>> Deborah Peel: Yeah. Well, I really disagree. I think the public is not in that place that they've agreed to give up their data for the greater good in the sense that you're talking about. In fact, we're seeing some of that right now with the kind of attacks that are going on for newborn blood spots. I don't know if you all know the situation in Texas. We worked very hard, Patient Privacy Rights did, with the Genetic Alliance and some great technology companies to try to get a consent process to be used rather than have the spots be destroyed. And, so, what happened in Texas was the newborn blood spot program somehow kept 5.4 million spots without clear authorization, and then they did use them in ways that turned out to be very disturbing to people, for various kinds of research projects without consent, and we need the newborn blood spot programs, and research has already shown that families are much more willing to share their information when they know that they're gonna be asked, the newborn blood spots in particular. You get -- you know, there seems to be a growing number of people out there that are terrified of research for I think completely unreasonable reasons, and we have to be able to address them and say, "No, you know, you're not gonna be forced to do this," and we need to be able to enable the rest of us that want research to say, "Yes, I want to keep those blood spots because if my kid gets cancer when she's 18, we can

compare the DNA at age 18 with the DNA from birth, and that will lead to some of the kinds of personalized treatment that you're talking about, but, you know, I'm very, very concerned that unless we get -- we return to the basis of research ethics, which is the autonomy of the individual and the individual's right to choose, we don't want to kill the goose that's laying the golden eggs. And just one other thing. In my field, again, mental health, 30% or 40% of the people are off the grid and there are no records for them. No records. So, I'm selfishly hoping that we can have a really trusted system so people who see therapists, who get treatment besides drugs, who -- with complicated mental conditions, so that we can actually know what the best treatments would be, and I know we'll never get it in my field unless there is truly a trusted consent system.

>> Manas Mohapatra: Kim, do you have some thoughts?

>> Kimberly Gray: Yes, thank you. Well, I think it's very unfortunate, to say it mildly, that these blood spots in Texas were destroyed. I think it's important to note that there was a disconnect in that particular situation in that, my understanding is, this was de-identified information, and I think where we really need to enhance things, other than necessarily through consent, is by enhancing public understanding of the difference, which is a significant difference, between de-identified information and identifiable information. The Texas case illustrates that lack of understanding by the public of just what can be done with de-identified information, and as Stanley had pointed out, consent is not always an easy thing to do when we're talking about research, and if we need to have the public good be the final goal of research, then we need some other alternatives, and maybe one good alternative is the use of de-identified information. I work for a company that does handle an awful lot of de-identified information. We receive roughly 75% of the prescription information in the United States in de-identified form. What comes to us is not someone's prescription information that identifies a person. Pharmacies are not selling us protected health information. But, in fact, we receive de-identified information, and then we treat it in such a manner that we put controls around that to avoid any appearance of re-identification, and we extend those controls not just internally but to external entities that might for some reason have reason to have that data. With using de-identified data, we're actually able to help not just commercial entities but nonprofits, state and local government, both. We work hand-in-hand with a lot of research institutions, big names that you'd recognize that are reputable institutions, such as Harvard, Yale,

MIT, Duke, UNC, Hopkins, and I could go on and on from there. We have shared information with Federal Government at the GAO, FDA, DEA, CMS and could I go on from there, too, but I'm offering another solution to the consent concern, which is let's use more de-identified information and let's use less patient identifiable information. It's patient protective to do so. It still enhances research and allows that free flow that others in the panel have also noted is so required. You have to have a free flow of information. We can't be stymieing research, we can't be stifling innovation, or we're missing all the goals of better quality, better outcomes, and enhanced healthcare in the new regime. Thanks.

>> Manas Mohapatra: I think de-identification is something that hopefully we're gonna have some time to address in regards to whether or not medical data or certain other types of data such as genetic data can truly be de-identified, but I just want to go back to -- I want to ask Marc, actually, are there alternative approaches in the research space aside from individual consent, such as the Ontario model or the recommendations I believe you worked on with the Institute of Medicine?

>> Marc Boutin: There are other models, and I want to stress the importance that there is no silver bullet to this. And I've said this earlier, consent is part of the solution. It's not the entire solution. The IOM recommendation was in essence to expand the HIPAA protections to all information in certain areas. The Ontario model allows for information to be provided to an entity that oversees how it's used for different research purposes. I think there are different ways to address this, but really at the heart of this is stratifying the issues both in terms of benefit and risk and then applying the appropriate solution to that metric, and I think that's the discussion we have have not had. The challenge is, again, people don't understand consent. As I said earlier, 75% of the population does not understand what consent means or how their information will be used after they give consent. We can certainly do a lot better in that space, and we have to, and there are models that have been utilized that have done better, but we still have not solved that problem. If you look at how health information is evolving, take, for example, the lack of awareness that the treatments that we receive on average work 60% of the time. Most people people with chronic conditions do not know that. 40% of the time you're essentially taking a placebo. For many complex conditions -- cancer or neurologic conditions -- it may only work 10% of the time. Within our lifetime, we're gonna solve that problem and figure out how to tailor the medicine so that we know it will work or

not work for you, but that's gonna come from research that's going to be at a large scale that is different from the kind of research we've done in the past that's gonna take a new model, and I can tell you, from the perspective of people with chronic conditions, they want this research to take place. They're still concerned about their privacy and security. They're still concerned about consent. But when faced with a life with a complex chronic condition and knowing that your children and grandchildren may face the same plight, you want that research to take place. So, how do we balance these competing options? Again, consent is part of it, but we they'd to look at how we stratify the risk, the benefit, and then apply the appropriate metrics, both in terms of privacy and in terms of safety. And, so, what that means is there's going to be different levels applied to different areas, and until we have that conversation as a society and figure out how to stratify that, we're gonna continually be at the spot that consent is the only solution and that privacy continues to be a problem and we continue to see people not seeking care out of fear and not get the solutions in terms of research that we all need.

>> Manas Mohapatra: Thank you. Jodi?

>> Jodi Daniel: Thank you. I agree that I think that a lot of our -- the benefits we're gonna see in the healthcare arena are gonna come from some -- from leveraging data that will now be made available hopefully and be more useful based on health information technology. The question is, is how do you then protect that information? And we're struggling with this, 'cause one of our goals is not only improve individual health and coordination of care but improve population health. One of the things I keep hearing that I think is really intriguing and that folks have experimented with is trying to keep the data close to the source, so that when an entity has a research question or a public health agency has a question about how a particular treatment is working or what's going on in a particular population, that they can send a query to the entities that are holding the data and get back responses without getting access to the individual data, and the FDA is doing this with their Sentinel program. There are other examples of this, as well, but it's a really interesting model for using data, not having that bias, but also not having the information flowing all over the place. So, it's, I think, a really good model to look at and see how much we can leverage that to both protect the data but also have the data that's necessary for research and get the results that the data can provide.

>> Manas Mohapatra: I have a question for Linda related to the research space. I know you had previously mentioned to us in our research calls the way that 23andMe had operated in terms of protecting the data but working with researchers to get results that they were interested in.

>> Linda Avey: Yeah. Well, it's a model that is -- and it's still sort of theoretical, but the idea is that having massive amounts of genetic data combined with phenotypic information that's been collected and layered on top of the genetics, when you talk to a researcher and they hear about that, they get real excited, and they say, "Oh, I'd love to have access to the data," but when you really probe them on it and get a little bit more information, it's like, would you really know what to do if you had access to the information? Would you know how to run the queries? Do you have a statistics background? Do you know the algorithms to run? And they stop short and say, "No." And if you even talk to people at the Broad Institute up in Cambridge, if you really ask them how many people truly have access to the data to run those queries, it's a handful. So, it's a very specific set of skills that people -- that a very few number of people have the ability to provide to an institution. That's a really -- you know, that's just the fact of the matter, and, so, if you've got researchers who understand a disease really well, they're not geneticists and they're not statisticians, but they come up with a really good query, then you can run that against the data and get the end result of that and then share that information back to them, and they're happy. They go off and they continue their research, but the data has stayed in this very safe environment. So, I personally believe that that's a very operable model, and when the NIH came out with dbGaP, which was this database where they were gonna -- because it was ironic that the NIH was saying, "Well, we're gonna come up with this very open-access model where you're gonna have access to all of these genotype data sets," and a group of individuals who were actually studying the forensics field were looking at whether if there was a pool of blood sample, multiple individuals, that you could pluck out the DNA of one individual, and they actually came up with a way to do that. Well, the same is true in In Silico data, that you can do the same thing, where if you pluck out a few bits of a person's profile, you can pull out their whole profile, and they pulled dbGaP down for that reason, because they realized there's no such thing as de-identified genetic data. So, it's worth looking at these models that people are coming up with, and we do believe that that is a very solid way to do it that protects people but also enables research.

>> Loretta Garrison: And, also, Kim, to go back on your earlier comments about the de-identified PhRMA data, or prescription data that you get, again, the protections that you apply to it and the controls that you apply to it, none of this falls under HIPAA. It is what your company does as a practice. Can talk also a little bit about what happens when you get queries to this -- to you for information about or access to the data? What are the controls that you want to place on that to the recipients and what, in some instances, are their responses?

>> Kimberly Gray: Okay. First of all, much of what we do is actually in report form. We're not actually giving raw data. We're giving reports that summarize it because, of course, we are the ones that do the statistical analysis, as opposed to the research, as was earlier pointed out. In those occasions, however, when a researcher wants particular information from us, we do impose the same kinds of controls on them that we would with anyone else who would want that particular information. So, for example, whereas internally we have security around the folks who are working with this de-identified data, only certain people have access to it. They're trained as to good practices around it. We extend those same requirements by contract to others, and we will occasionally get push back from researchers who don't want to play in the same playing field that we're paying in. They don't get that information, that that is a requirement. So, for those few researchers that don't want to play ball with us, we will not be sharing the information, but I must say that most researchers are not looking for that anyway. They are looking for the aggregated information because they don't have the statistical ability, and it's much more useful for them to have the aggregated data tables, and those controls would be onerous in some cases to put on individual researchers who are not necessarily affiliated with the larger institutions.

>> Loretta Garrison: Jamie, quickly.

>> James Heywood: Well, I think we want similar systems to 23andMe and, I think, IMS, in that we sort of retain the data, we run the queries, we'll ask the questions, and we've struggled with this question, because I think we have a trust relationship with our consumers, and we impose the same trust restrictions which we, you know, are non-re-identification and discrimination on our partners. But, actually, I'm really uncomfortable with the use of the word de-identified. I mean, I think it's --

I will tell you, if you look at the 10,000 of our patients that are public, you could, with 100% accuracy, pattern-match them to your system, and there's no question that that's possible, and it's a query you could run on patients that are putting public information in their profile. So, I think that we should -- you know, we have to be honest about this question. If you have four data points about a patient, I mean, even the implication that a genomic spot, that, you know, the date of birth and the gender and the city, that that's de-identified, I mean, there's no more specific identifiable data in the world. So, under those conditions, I think we really are talking about this question of a trust framework, not a de-identification framework, and I certainly would not pretend to our customers that the information is de-identifiable. In fact, we explicitly say that it can be re-identified on the website in three FAQs. So, it's very -- this is a very -- I think it's a very, very dangerous term that we should use at all anymore.

>> Loretta Garrison: Okay. What I'd like to do is to give each panelist about a minute to reflect back on all the issues we've discussed today and just present two or three key points that you think are most important. And we'll start at the far end with, I think with Marc.

>> Marc Boutin: I'll just conclude by saying that we have a long history of protecting privacy. We also have a long history of promoting public good and social interests. And there's been a balance between those two competing aims historically. The balance ebbs and flows, depending on the context of where we are as a society, and I think we're at one of those critical points in time where society is changing. Technology is changing. Information is changing. Health and the way we deliver health and the way we develop treatments are all changing. So, we're at a pivotal point in our time, so it makes sense that we're having this conversation. I think the challenge is, again, to get the balance right for our current needs and realize that it is not a zero-sum game. Privacy is not gonna totally trump social need. Social need or social good is not gonna totally trump privacy. The challenge is to get the right balance given our opportunity both at the individual level and at the societal level. So, I thank you for taking the time to listen to me.

>> Loretta Garrison: Kim?

>> Kimberly Gray: Two points. First of all, the de-identification point, and I'm not going to disagree with Jamie that things can be re-identified. However, I think that Jamie makes an important point in that he notes that these are publicly available points. His work is done via a public vehicle, and I think as long as we are not -- and any previous re-identification that's been published has all been because of publicly available information. I think the important thing to do is to ensure that your controls, if you're working with de-identified information, are not just your internal policies and procedures and your oversight, having your privacy office at your company and your security safeguards, but that further step of restricting anyone downstream from re-identification, and if there is re-identification, have penalties for it. Actually have CNPs or whatever it happens to be that if somebody's going to go to that extra step by co-mingling with publicly available data and doing a re-identification, they should suffer the consequences for that, and then, internally, continue to reassess your processes to make sure you're keeping pace with technology and that you're not allowing that same thing to happen, which is my segue into point 2, which is be accountable. IMS is not a covered entity, and we are doing things that we've chosen to do because we are an accountable organization and we do care about patient privacy and we also care about research and all the public good that's coming from it. Accountable organizations take this organizational commitment from the top. They put their internal policies and procedures in place. They have privacy protection goals that consider many things -- laws, public policy, best practices, and self regulation -- as a part of that. They do training and education. They believe transparency. They demonstrate that they can do what they say they're doing, public education about what they're doing, and then, lastly, mitigating any harms if there should be one that occurs and taking their lumps as a final step being enforcement. And this accountability principal is one that's not new, and it's global, and I think we need to think globally, 'cause privacy is global. Many of us are in global companies, but bottom line is privacy is global and the accountability principle started with OECD. The EU has it, PIPEDA in Canada has it, APEC has it, and even Gramm-Leach-Bliley to some extent has it, because it all says, "Here's the end where we want to get. Our means may differ as to how we get there, but back to that whole trust thing that's permeated this panel discussion today, if we have accountable organizations that go down this pathway, we've got the trust that's needed by consumers.

>> Loretta Garrison: Thank you. Deven?

>> Deven McGraw: We absolutely have to make sure that personal health information is protected wherever it is, and we have some protections for it, whether it's in the healthcare system, and we don't have them when it leaks out or is voluntarily put up by consumers. So, at a minimum, we can count on accountable organizations to some degree, but there are a lot of organizations that are taking advantage of a rule-free environment, and they're, quite frankly, gonna spoil -- upset the apple cart for those who are accountable. So, at a minimum, some baseline rules that apply consent should play a much bigger role because this is a consumer-based world, and to some extent, what they would want to do with their data, they ought to be able to do with their data. We need to be much more clear about telling them what the risks are, not just buried in privacy policies, but through other techniques and devices that can get consent in a more clear and obvious way, but we can't just count, in fact, on consent. As many people have said very well today, it's an imperfect protector of privacy. Nice alliteration there. So, as a result, we also need to look at what might be patently unfair to consumers that's going on on there for which the FTC actually already has jurisdiction to crack down on.

>> Loretta Garrison: Jamie?

>> James Heywood: You know, this is to my mind a much bigger question than privacy. I think, you know, we stand at a moment in time where the sort of very fabric of our modern society is being challenged by technologies that are connecting us in new ways, and I think that the choice that we have to ask ourselves now is, how do we approach this problem? And while many of the technical details of this I think I agree and we could disagree with, but I think there's a principle that I want to elevate up one level, which is, what kind of world do we want to live in? Do we want to live in a world that is transparent, that is open, that is collaborative, that is honest, or do we want to live in a world where, you know, we are preventing the flow of the blood of humanity, which is information, because we have so weak, we have chosen not to address discrimination? And I think this choice now is between a hard and an easy road, and the easy road is to say, "Oh, discrimination is bad. Let's make sure that anyone that makes any information flow anywhere that makes discrimination happen is punished," 'cause it's easy to punish people that deal in information. The hard road is to actually live to the principle that all are created equal and incorporate it in law

and make discrimination not happen so that the consequences of the flow of information go away so that stigma, which is the problem we're talking about, goes away because people come into light with issues and that we collaboratively solve problems as a society. And I think we don't face this choice well. We're making the decision to look at information and not discrimination, and I think we should really look and ask ourselves, what world do we want to live in as we develop these policies?

>> Loretta Garrison: Thank you. We are the only ones standing between this group and lunch. So... Deborah.

>> Deborah Peel: Okay. I'll try to go quickly. Yeah, I appreciate what you're saying about the wider question and what kind of world do we live in, and I think most Americans want to live in a democracy, and the fundamental, most important personal liberties and personal rights have to do with being able to be separate and not have everything be known about you. I think in the words of Supreme Court justice Brandeis, I think he said the highest rate of civilized man has the right to be let alone. The right to have privacy is essential to democracy. And I really appreciate -- I think that actually there's a lot of agreement on the panel that the ability to consent is very important and that individuals should make choices, but I would just like to point out that consent is not in the meaningful use criteria for all of the EHRs that are gonna be purchased to start this connected world. We don't have the ability to control the information currently. And, so, that's a really important point, and since this panel does agree that some degree of consent is needed, you know, maybe you can help us work with the agencies and make sure that gets in there. I know our coalition wrote a letter and asked the Health IT Policy Committee to be sure and put consumer controls in up front, and they're not. They're at the very back. So, that's really important to understand. And then, in terms of things like trusted organizations, at some point, we're gonna need an external trusted consumer organization that can evaluate the claims of all of these companies, whether they really do what they say or not, because it really is impossible for individuals to figure it out. And, so, individuals have rights, and as you think about this, I hope you'll think about who you think can make the best decisions for you and your family about your sensitive health information.

>> Loretta Garrison: Thank you. Jodi?

>> Jodi Daniel: Thank you. I believe that we need a privacy and security framework that applies to all entities that hold information and that we need to do a better job of preventing and addressing harms, as Jamie had mentioned. I think we need to do both. I think the fact that we have uneven protections is a problem because it affects trust. So, if a patient assumes that when -- that information's protected because there is some law in this space, the HIPAA laws -- and don't understand that it might not be protected in another environment and that information is used in a way that they didn't anticipate, it erodes trust. And I think if we don't have this framework, we're not gonna realize all of the benefits that we can realize, both from consumer engagement from having better information to help support research, et cetera. We're doing a couple things I just wanted to quickly mention. We do have a privacy and security framework for health information exchange, the HHS, that ONC released in December of 2008, which tries to focus on fair information practices, including consumer choice and transparency. We're working on a model online privacy notice that folks could use to help improve transparency as to how information is being used, and we're also looking at how to protect information held by non-covered entities. This is something that congress required us to do under the HITECH Act. And we're also looking at consumer-choice policies through our privacy and security policy committee, et cetera. The issue here is that all of these things we're doing are voluntary. I mean, these are not -- we're not talking about, you know, a government mandate to protect information in these certain ways. And I think we do need to think about how we hold people accountable and make sure that there is an even framework so that there are, you know, some actors who are trying to do the right thing and others that are blatantly using information in ways that folks would not understand or anticipate and don't -- and not communicating that to folks. So, that's -- that's it.

>> Loretta Garrison: Thank you. Thank you. Linda?

>> Linda Avey: So, I agree with everything everyone else is saying. So, one of the things that I think would be really interesting to look at is could the government be in a position to really point out success stories? Where -- where have we seen companies that have done a really good job, who have shared information and enabled consumers to get their information out and where it's

been used productively? Because I think we talk in theoreticals when we talk about all of these harms and the scary stuff. The story -- you know, when somebody loses a computer with a database on it, that was the story? You know, what happened? What was the implication from that? What was the result of a computer with information on it being lost? We don't ever really challenge these fears that people. They're just sort of unknowing, but they think that sounds scary, and I think that's why they answer surveys and they say, "Oh, I would never want my information out there," but nobody ever challenges them on that. But, instead, if we can turn this whole thing around and say, "Here's a situation where people shared information and here's a really positive outcome that came from that, and let's reward that behavior." And then, certainly, as Stan was saying, if we know places where people are not following what they say they're gonna do and they don't abide by their own self-imposed rules or others, that they are persecuted -- or prosecuted. I'm sorry. [Laughter]

>> Deven McGraw: We should persecute them!

>> Linda Avey: [Laughing] Yes, yes. So, you know, we have laws in place that allow us do that, and I think the government has things to challenge companies that are the bad actors, but let's not put everybody in the same bucket and really reward success if we can.

>> Loretta Garrison: It's much easier to challenge when you have standards.

>> Linda Avey: Exactly.

>> Loretta Garrison: Stan?

>> Stanley Crosley: You know, I'm stuck here with the traditional and nontraditional concepts, as well, and I think, within the traditional concepts, there are easier solutions where, for research and things, where we look at public benefit and we see a societal benefit and improvement to individuals' healthcare and quality. I think uses can be better understood, and I think we can -- we can move to models, like Linda suggested, models that, in fact, Ontario has with trusted entities, or even the FCRA. Right? I mean, they have a trusted entity concept on access and utilization of

information. Not everybody gets access to the information. So, I mean, I think those are models that are valid. I think the IOM report talked about some of those. The nontraditional setting is much tougher. It's much more difficult, and I think Jamie, you know, set out the concept of how transparency is just ultimately so critical, and I couldn't agree more with that. I also believe that the table stakes, regardless of whether it's traditional or nontraditional, is security. I mean, I don't think there's any excuse whatsoever for not having appropriate security around the health information. I mean, I don't care where it is or who has it, and I would be in favor of understanding how some type of a framework could address the security issues. Control is a much different and much more difficult concept, and I think we need to keep working our way through it.

>> Loretta Garrison: Terrific. I want to thank each and every one of our panelists for a very stimulating conversation. Thank you. And -- [Applause] When do we come back? You have a break for lunch.

>> Male Speaker: 1:45.

>> Loretta Garrison: Please be back at 1:45. Thank you. Thank you so much.

>> Deborah Peel: Absolutely.