FTC Spring Privacy Series: Consumer Generated and Controlled Health Data
May 7, 2014
Transcript

CORA HAN: --to check in with the person accounting for everyone in the conference center. In the event that it is safer to remain inside, you'll be told where to go inside the building. If you spot suspicious activity, please alert security.

This event may be photographed, videotaped, webcast, or otherwise recorded. By participating in this event, you are agreeing that your image and anything you say your submit may be posted indefinitely at ftc.gov, or on one of the Commission's publicly available social media sites.

If you would like to submit a question, question cards are available in the hallway immediately outside of the conference room. If you have a question, fill out your card, raise your hand, and one of our paralegals will come and get it.

For those of you participating by webcast, you can email your question to Consumer Health Data at ftc.gov, Tweet it to #ftcpriv or post it to the FTC Facebook page in the workshop status thread. Please understand that we may not be able to get to all of the questions.

So now I would like to welcome Commissioner Julie Brill to the podium for some brief welcoming remarks.

JULIE BRILL: Thanks, Cora. I want to be really brief because this is a great topic. First of all, it's great to see so many of you here, and thank you for all of you who are watching on the web.

This is an incredibly important issue. Those of you who know some of the things that I talk about when I go out and speak and write know that this is an issue, the issue of consumer generated health information, is one that's near and dear to my heart.

So let me just very briefly paint the big picture and talk about the benefits and some of the concerns, which I know you are all thinking deeply about and I hope you will keep in mind as the day progresses.

Big picture, consumer-generated health information is proliferating. Not just on the web, but also, of course, with respect to connected devices, the internet of things, or that Cisco says so famously on all the TV shows that I watch, the internet of everything.

The potential benefits to consumers are significant. The potential benefits to society are incredibly significant. But also, there are some risks, I believe, and I hope we will talk about today, with respect to health data flows that are occurring outside of HIPAA, outside of the medical context, and therefore, outside of any regulatory regime that focuses specifically on health information.

Some of you know, because you were there as well, I was at the Consumer Electronics Show in January, and was really wowed by much that I saw. Some of the devices that I saw were particularly focused on health, and the measured life, quantitative life.

One in particular that really struck me was the Memo. It was a onesie that was developed to measure the heartbeat and respiration rates, and other vital signs, of an infant, a newborn. And it could send information to an app, it could send information to the parent's mobile device and whatnot.

And think about the benefits of anyone who's worried about SIDs, any parent that might be worried about SIDs, or just might want to get their baby to sleep better or get themselves to sleep better. Monitoring some of these important vital signs would be a real benefit in all of those areas.

We've seen tons of wearable step counters, mileage monitors. There have also been some interesting articles about doctors who are finding out more about their patients by going online, googling them. There was a New York Times well blog post on that. Or an interesting ethical debate underway in the medical community about whether doctors should become friends with their patients on Facebook or other social media.

And then, of course, another topic, which I'm sure will be discussed today, is the now infamous example of companies that are generating their own health data about their customers based on purchases, such a Target did with respect to its pregnancy predictor score.

So again, taking a step back, thinking of the significant benefits that consumers can gain from some of these devices and their ability to measure their health conditions and whatnot.

They can monitor their health, they can monitor their family's members health in the event that they have an elderly parent, or, again, the young child. They can find motivation to exercise or eat healthier foods. They can connect with people who have a similar medical condition or disease. They can participate in research. All incredibly beneficial.

But, again, when health data is stored outside of silos, outside of the HIPAA silo that was created a fairly long time ago now. It seems like eons ago in terms of the digital age. It will be health data that is not being controlled by doctors or hospitals or insurers.

I think when you look at HIPAA and you look at high tech, for instance, there seems to be consensus in this country that health data is sensitive and does need special protection. And then the question becomes, though, if we have a law that creates these protections but only when they're flowing in certain contexts.

But the same type of information or something very close to it is flowing outside of those silos that were created a long time ago, what does that mean? And are we comfortable with that, and should we be thinking about breaking down the legal silos in order to better protect that same health information when it's generated elsewhere.

Of course, there's also the problem of re-identifying individuals through information that had been de-identified. Latanya Sweeney, we're not going to necessarily talk about today, but we so loved having her here at the FTC. She's one of the nation's experts, as many of you know, on that very issue and so many other issues.

There's some interesting things that I've read about, and I don't know if people will be talking about this today. But we recently read that one insurance company, Aetna, has developed and app for its beneficiaries to use, where it will allow consumers to set goals, track their progress on all sorts of health indicators-- weight, exercise, things like that.

Now, it's wonderful that Aetna set this up. I think it's great. But I don't know precisely what they're doing with this information. We've looked at the terms of service. It just raises interesting questions to what extent could this information be used for rating purposes. And we all know that under the FCRA it ought not to be. But what are the rules of the road here.

The other interesting example that I remember reading about recently was an entity called Blue Chip Marketing, which was being used by pharmaceutical companies-- or being hired by pharmaceutical companies to help them find candidates for clinical trials.

Now, Blue Chip Marketing was not a doctor or it didn't work with doctors, it didn't work with hospitals. Instead, it surfed social media, it surfed cable TV subscriptions, and got lots of information that allowed it to infer whether consumers were obese, potentially had diabetes, and potentially had other medical conditions. And then offered to them to join a clinical trial.

Now, some consumers would think that that's great. Yes, I'd like to be part of a clinical trial. But other consumers were really shocked when they got contacted by this company or others that got the information from the company saying, what makes you think I'm obese, or how did you know I was a diabetic? Really interesting issues.

So, again, I'm really looking forward to the day. I'm going to sit here as long as I can, and I'll say hello to as many of you as I can during the breaks. But my plan is to sit here, and I know there will be a deep discussion about all the new health data that is being generated by new devices and new online services and apps.

I know we'll be exploring the benefits because the benefits are significant. I do hope we'll also explore the risks. And I would like everyone to keep in mind that health data, from my perspective as one commissioner, is highly sensitive, even though it may not be created and operating within HIPAA context.

So with that, I'm really looking forward to the conversation. And thanks so much to Menitia, to Cora, to Kristen, and to others for organizing this great day. And welcome to all of you. Thanks.

[APPLAUSE]

CORA HAN: Thanks, Commissioner Brill.

So to begin the program today, we're going to start off by a presentation by FTC Chief Technologist Latanya Sweeney on health data flows. Let's welcome Latanya.

LATANYA SWEENEY: It's great to be here. And I, too, want to thank Menitia, Cora, and Kristen for having me and giving me this opportunity to speak. There's kind of a duality in this talk. I absolutely love being at the FTC.

But most of you know that my real job, in a sense, is at Harvard, a professor. So the work that I'm going to talk about is actually work not done at the FTC. But that certainly I had some intersection points with respect to this workshop.

So for that reason, I have to start out with a disclaimer that anything that I say is not the views of the commissioners or of the Commission, and I have to tell you they're also not officially my views.

[LAUGHTER]

So I want to talk about the relationship between transparency and trust. Individuals have, as Commissioner Brill made such a great point of talking about the fact that individuals have control of their own data. The data that they can generate, the data that they might pull out of the HIPAA system, in the sense of asking for that data from their physician and so forth.

And what they can do about it is up to them. And one of the things we all want is for them to live their lives better with that data.

The question that gets posed from the kind of work I do is if you have that kind of control over your information, how do you make decisions, and how do you know that those decisions won't cost you harms? After all, how did their decision-making compare to a lot of the regulatory type decision-making is one of the questions.

And so my slide just messed up, because welcome to the world of PowerPoint. So I'll just skip ahead.

So I think when we think about health data it's really for most people it comes down to the relationship between the physician and the patient. If there's not trust in that relationship, then the physician doesn't get all the information, the patient may hold back information. And if the patient holds back information, they risk not getting good care.

So I think we all understand the need for a kind of transparency and honesty of information going there. But what we don't always know is where the data goes after it leaves there, independent of other places an individual might place the data.

So a couple years ago we started a project at Harvard called the datamap.org, and our goal was to try to document all of the flows of data. After all, health data's been going around for a long time. Where are all the places it goes? And to our shock, it's really not clear. It's not easy to know all of the places it might move.

So we used all kinds of devices-- mining web pages and notices, mining breach notices, and breach notice databases. And also issuing public requests. So if there was a government agency that was somehow getting the data, we would then issue a public request to ask to whom did they give it, what's the data, and so forth.

Now, we weren't the first group to try this. In 1997 there was a commission headed by Paul Clayton at the National Research Council who attempted to do this, and this was right in the middle of the HIPAA debates. And they sat down, and through the committee, began documenting all the places that health data may go.

And it's kind of interesting. This is a model of their graph. And you see all of the places that you might think, and some of them might be a little surprising.

So with our efforts, this is what it looks like today, sort of eight years after HIPAA. And what you see not only is explosion in the number and types of data being given away, but there's also just different kinds of entities also receiving the data.

If you visit the datamap.org, you can actually click on any node and it will give you actual instances of how we came to know that. It'll give you the company and what it is that they're doing.

Another question, once we had this map, we began asking questions. So one of the questions is which of the flows are covered by HIPAA and which are not? And to our surprise, about half of the flows are not even covered by HIPAA.

So right away we saw an interesting issue that when you ask-- certainly when we surveyed students, the students said they expected most data outside the data they give themselves to be covered by HIPAA, and we found that most were not.

One of the critical pieces there that you see is sort of in the middle there called discharge data. So we began to focus on that. We see a lot of pieces going out, and for most people, what the heck is discharge data anyway? Whatever this discharge data is, it starts from the patient, goes to the physician of the hospital, and then it comes to this discharge data.

How many people have heard of discharge data in this room? OK, so that's about half. So whether you've heard of it or not, if you've had a hospital visit, and in most states are physician visits, information about your visit is in discharge data. These are mandated by state laws. A copy of that data goes to whoever's designated by that state law to receive that data.

And what you're seeing here on the data map is not just that they got the data, but you also see that they're either selling or giving away that data to others.

The dashed line means that they did so in a way that didn't have your explicit name, but it was, in fact, de-identified. That is, it didn't have name, address or social security numbers, but it included diagnosis codes, procedure codes, and how you paid for it.

So, in fact, 33 states sell or share personal health data, and this is a list of the states that do so. And then we said, OK, so they're getting the data. They're selling it. They're sharing it. But how many of them adhere to HIPAA? And it turns out only three of them do.

The other states are sharing and giving the data away in a way that's less protective than HIPAA. They're less protective in the way HIPAA would describe how you might share or sell personal health information.

So one of the questions then is well, maybe HIPAA's just too strong. Maybe the federal standard is just kind of too high, and that there's nothing wrong with the lower standards that many of the states are using. Or is it the case that the states should actually change their practices and perhaps raise the standard to the HIPAA standards for the stuff that they commonly give away or share or sell.

And then maybe have some other alternative if people needed more sensitive data. So to test it, we went back to the data map and began to ask the question, also, what might be harmed if any of these questions posed out to be true?

So one of the kind of interesting loops we found was this loop to financial companies. So the data goes from you to the physician, and from the physician to the discharge data, and then to a bank. That sounds really interesting.

So we looked at the literature, and many years ago, there was this article in the New England Journal of Medicine that described a banker who cross de-identified health data about cancer patients in an attempt to figure out if any of them had mortgages or loans at their bank, and then begin tweaking people's credit worthiness.

Now, I have no idea if that's true. But if we could show that it's possible by asking the question, that dashed line, how de-identified is that data? Is it sufficiently de-identified?

Another question comes up is the online websites. You give information to the physician and the hospital, you give information to an online website. To what extent are the websites who are receiving the discharge data re-identifying you to the medical data that was left behind.

And so this becomes a real interesting question because at the time you're giving the data to the online website, you would have no idea what other data they may be pairing with it or what they might know. And if you click on the online website, you might see some of the companies.

So as I said, we gave out these four year requests for the top buyers, and we listed the top buyers across the states. And it's kind of a surprising list. You see a lot of analytic companies that most people have not heard of. We see WebMD who has a large online website. We see IMS Health who uses a lot of pharmacy data. We saw also unions, which is kind of-- I don't know the story of that. Clearly, there's a good story there.

So let's figure out how de-identified is this data. Is it safe? Is it OK the way they're getting it out. So for $50 we went to the State of Washington and we purchased their hospital discharge data for the year 2011.

And what you see here is just a sample of the 300 and some odd fields of information for each visit. It included the age in months and years, gender, zip code, and then you can see sort of what happened to the person, what hospital they went to, how they pay for it, and so forth.

At the same time, we wanted to find a way to figure out how we might re-identify individuals to look at the kind of thing a banker might know about a person who had mortgage at the bank. In other words, to what extent would that New England Journal of Medicine, could it really be true? Could a banker do it?

Well, a banker and an employer and others know the same kind of information that often shows up in news clips about accidents. So we took one news source in Washington State and just surveyed that one news source for news articles that contained the word hospitalization or referred to hospitalized. And we got 81 samples.

And the typical story is like the one you see here that often includes the age of the person, the city in which the person is coming from, where the accident happened. A lot of times it'll include the hospital and a description of the accident. But it doesn't include the zip code, which is what the health data.

So what you see on the left is we just went to public records given a person's age, their residence, and their name. What are zip codes associated with that person? And these are just common public record sites.

Then we did the thing on the second. We take the stuff that we had from the news story with the zip code, and we look for an exact match. Means I'm going to take the fields, I'm going to try to match exactly those fields.

If I get one and only one match, we feel pretty confident that's the person, because state-wide collections is everybody. And if we didn't get a match, we would relax one field and see if we then got one and only one match, because there could be errors in the news story.

And we were able to exactly matching-- this is not statistical-- 35 of 81 of the news samples, or 43%. And that's exactly the same kind of information an employer would know about employee taking time off, a creditor would know, family, friends, or neighbors might know.

So let me stop there. Hopefully I've inspired you to think about some of the issues and questions that come up when individuals are sharing their data. The goal here is not to say that individuals shouldn't. But the goal is to figure out what are the risks and then jointly move forward about what do we do to move forward with the benefits while addressing the risks.

Thank you.

CORA HAN: Thanks, Latanya.

[APPLAUSE]

CORA HAN: Thanks. So next I would like to take a closer look at some data sharing by select health and fitness apps with a presentation by Jared Ho, who is an attorney in the FTC's Mobile Technology Unit. Thanks.

[APPLAUSE]

JARED HO: OK. Before we get started, a special thanks to Tina Debokaro and the mobile lab for their support and expertise. To Cora Han and Kristen Anderson for putting this show on. To DPIP and the Mobile Technology Unit for their keen insight and input into this project. It was truly a collaborative effort.

So to get started, we started with the understanding that consumers reveal significant amounts of information about themselves when they use health and fitness apps. So this includes everything from basic information about the devices and smartphones they are using, to the precise metrics and characteristics of their bodies.

So when we're talking about health and fitness apps and the wearable sync to those apps, those characteristics and metrics might include everything from running routes, to eating habits, to sleeping patterns, the symptom searches, and even the stride or cadence of a person's walk or run.

Under this backdrop, we'll take a look at a couple of studies that have already been conducted in this field. In July of 2013, Privacy Rights Clearinghouse examined 43 free and paid apps. They examined the privacy policies of those apps, as well as tested the data transmissions of those apps.

They ultimately found that a large percentage of the apps did not have privacy policies. That about a third of the apps transmitted information data to a party not disclosed by the developer or the developer's website, and only about 13% of the apps encrypted all the transmissions between the app and the developer's website.

They ultimately concluded that health and fitness apps were not particularly good at protecting consumers' privacy. Since we did not review the privacy policies of any of the apps in our snapshot, we do not express any opinions as to Privacy Rights Clearinghouse's findings or conclusions.

Moving on in September of 2013, Abingdon conducted a similar study. They tested 20 health and fitness apps and found the presence 70 third parties. They found that these third parties were typically advertising and analytics companies.

So this graphic is actually a picture of three third parties that received information from 14 different apps from the Abingdon study. The blue dots represent the third parties, and the cell phones represent the apps.

So who are these third parties? What kind of information are these third parties receiving about our bodies? And does the picture actually look different if we include wearables?

So we designed a snapshot to try to find out and take a deeper dive. So we looked at 12 health and fitness apps on one operating system. Two of those apps where apps that allowed us to sync information with our wearable devices.

We tried to take a broad range of apps that gathered a variety of metrics about our bodies. This project was meant to be a small snapshot in time, so we looked at two daily activity apps connected to wearables. Two exercise apps to dietary and meal apps. Three symptom checker apps, and one pregnancy app, one diabetes app, and one smoking cessation app.

So using our mobile lab, we examined the information being transmitted from each app. While interacting with each app we were as permissive as possible. Meaning that if an app asked us for permission to access a certain feature or to sync with another app, we always accepted and opted in. We then mapped out the data sets to visually see the types of information being transmitted from each app and to whom this information was going.

So a few limitations. We limited our snapshot to one mobile device, and, therefore, one operating system. Our snapshot was limited to free apps, so we did not test any paid apps or if an app had premium features we didn't purchase those features.

We only examined the data transmissions between the apps and the third parties on the front end. Meaning while we were interacting with the app, while additional information collection and sharing can certainly happen on the back end, our snapshot wouldn't have captured that.

And again, we did not review any privacy policies. So we don't make or express any opinions as to the actual information collection practices or sharing practices of the apps themselves or the third parties.

So onto the snapshot. We started with 12 different apps. During our testing we found that these 12 apps transmitted information to their developer websites, which are represented here by the yellow dots. Our testing also found that additional information was transmitted to 76 third parties. They're represented here by the blue dots.

So what does this graphic mean? Zooming in and taking a closer look at one app as an example, we see that this app transmitted information to 18 different third parties.

These third parties received a variety of information that generally fell into five categories. Device information, such as screen size, device model, or language setting. Device-specific identifier, such as a UDID. Third party specific identifiers, which you might think of as are a

cookie stream specific to a particular app. Consumer-specific identifiers, and consumer information, in this case, dietary and workout habits.

So looking at it from another direction we might ask ourselves what information are these third parties receiving from a variety of apps. So this was an example of a third party ad servicing company that's received information from four separate apps. We found that the same unique identifiers were transmitted to this third party from the various apps.

We found that the apps also transmitted additional information to this third party, such as at least one at transmitted keywords such as ovulation, fertilization, pregnancy, and baby. So that essentially identified the type of app that it was to this third party. At least one app transmitted gender information. At least one app transmitted workout information. And all of the apps transmitted basic information about our device.

So while the third parties received the same identifiers that uniquely identified our device between apps, we don't actually make any determinations as to what this third party did with the information that it received from the various apps.

So moving on to our first observation. We found that 18 of the 76 third parties collected persistent device identifiers, such as a unique device ID, a Mac address, or an IMEI. In some instances, the same third party received the same persistent identifier from multiple apps.

Our second observation we found that 14 of the 76 third parties also collected consumer-specific identifiers. In most instances this was a user name. A few instances we found a name and email address being transmitted. It wasn't uncommon for a third party or an app to identify a user by their first name, a last initial, and then a string of identifiers.

And our third observation was that 22 third parties received additional information about our consumers, such as exercise information, meal and diet information, medical symptom search information, zip code, gender, geolocation.

And finally, a summary of our observations. Health and fitness apps collect and transmit to third parties sensitive information about our bodies and our habits. The 12 apps that we tested transmitted information to 76 third parties. The information included device information, consumer-specific identifiers, unique device IDs, unique third-party IDs, and consumer information such as exercise routine, dietary habits, and symptom searches.

So there are significant privacy implications where health routines, dietary habits, and symptom searches are capable of being aggregated using identifiers unique to a particular person or their device.

Thank you.

CORA HAN: Great. Thanks, Jared.

[APPLAUSE]

And now I'd like to welcome our panel up to the stage, and we'll have the panel part of this.

KRISTEN ANDERSON: Good morning, everyone. My name's Kristen Anderson, and I'm also an attorney with Division of Privacy and Identity Protection. Cora Han and I will be co-moderating this panel.

So our discussion this morning will focus on the ways in which consumers are generating and managing their own health data. We'll hear from our distinguished panel of experts who all have different perspectives and varied experiences about how consumers are going about this, what some of the risks and benefits are, and what they think the next step should be to encourage innovation while protecting consumers' privacy.

So we're joined today by Dr. Christopher Burrow, who joined the Humetrix Executive Team in 2010, and is the company's principle Data Security and Privacy Officer.

He's a physician, scientist, and biotechnology executive entrepreneur in the field of genomics and personalized medicine. As a clinician and health information data specialist, Dr. Burrow has played a key role in the development of Humetrix Blue Button enabled mobile apps, including iBlueButton and ICEBlueButton, working closely with the software development team.

Next we have Sally Okun who is Vice President for Advocacy, Policy and Patient Safety at PatientsLikeMe where she's responsible for patient voice and advocacy initiatives. Participates in health policy discussions at the national and global level. Oversees the company's patient safety initiatives, and acts as the company's liaison with government and regulatory agencies.

Next we have Joseph Lorenzo Hall who's the Chief Technologist at the Center for Democracy and Technology. His work focuses on the nexus between technology, law and policy, ensuring that technology and technical considerations are appropriately embedded into legal and policy environments.

And finally, we have Joy Pritts who joined the Office of the National Coordinator for Health Information Technology, and the Department of Health and Human Services in February of 2010 as its first Chief Privacy Officer. Ms. Pritts provides critical advice to the Secretary and the National Coordinator and developing and implementing ONC's privacy and security programs under HITECH.

And unfortunately, our final panelist who was supposed to be here today is Heather Patterson, but she's been unable to join us. So we'll miss her input, but Joe Hall's actually familiar with some of her research, and will do his best to speak about some of her findings, and our other panelists will fill in as well.

CORA HAN: So thanks to all of our panelists. We'd like to start by setting the stage with why we are having this discussion about consumer generated and controlled health data.

As Latanya Sweeney noted in her opening presentation, HIPAA doesn't cover all health data, but consumers may not know that. So Joy, I'd like to start with a question to you. Could you sketch

out the boundaries of HIPAA for us? And describe under what circumstances a consumer might generate health data that wouldn't be covered by HIPAA.

JOY PRITTS: I'd be happy to. Thank you.

Many people, not probably most of the people in this room, but laypeople think that HIPAA covers all health information. They are familiar with getting the notice in their doctor's office. And they also receive notices from people who aren't covered by HIPAA saying, we follow HIPAA.

But HIPAA actually is pretty sector-specific. And by that, I mean in this country the way we regulate information really applies to the people, for the most part, who hold the information, or who generate the information. And in this case, HIPAA originally applied to health plans, most health care providers, and these things called health care clearinghouses that were kind of essential to the transmission of claims data.

One of the interesting things about HIPAA that many people don't realize is that it really generated from a movement to a standardized claims data. It wasn't really about privacy at all originally.

Privacy was included as a protection, but the focus was on simplifying the administration of health claims and how they were processed. When you know that, a lot of what happens under HIPAA makes a whole lot more sense.

So the way it works is that HIPAA directly applies and directly regulates most of these health care providers and health plans. And it puts limits on how they can use and disclose the information. So it really focuses on who holds the information, and what they can do with it, and who they can share it with.

The general rule is that they can't share it, except under certain circumstances-- without the patient's permission, except under certain circumstances. And there are a lot of exceptions under HIPAA which were aimed at trying to make the core purpose of providing health care and payment for health care easy and simple. So you have health plans and health care providers.

And under the relatively recent enactment of the Economic Recovery Act, there is a piece in there where Congress also improved the privacy protections, and that was referred to earlier by Commissioner Brill as HITECH. And under that Act, Congress expanded the privacy protections.

So you now have a situation where it's not just the health plans and the health care providers. But the protection also of HIPAA flows to people and organizations that undertake really core activities on behalf of those, what they call covered entities and business associates.

So under HITECH, the data map that Latanya showed us a little bit earlier, it still presents a very interesting diagram, but there would be more solid lines, a few more solid lines. But they also depend on what function that organization is performing.

So, for example, in that map, Latanya had an arrow that went to lawyers. Well now, if a lawyer is performing a service on behalf of a doctor, for example, then they must also follow the HIPAA rules for privacy and security.

On the other hand, if a lawyer subpoenas those documents for another purpose, it's not protected by HIPAA. So you can see that it's a little complicated for people, and particularly laypeople, to understand how this works because whether health information is protected depends on who's holding it and for what purpose.

CORA HAN: Yeah. No, that's great. So could you describe a situation, for example, in which a consumer might unwittingly cause HIPAA protected data to sort of move outside of the HIPAA bubble?

JOY PRITTS: Well, we're actually trying to encourage them to do that. So that's a very interesting situation.

One of the rights that individuals have under the HIPAA privacy rule is a right to get a copy or to get access to their own health information, and that includes getting a copy of that information.

HITECH contained a provision which really clarified that individuals have a right to get an electronic copy of their information when it's available. We think that this is a really important aspect of health care as we go forward. Because under the Affordable Care Act, patients are really being put the center of their care.

We're trying to move from a paradigm where health care is just provided on an episodic basis, and really treat the patient more holistically. But what that means is in order to do that, you need information going back and forth between a doctor and a patient that is related not only to their doctor visit, but also how they're living and what they're doing in the outside world, because then you get the entire picture.

One of the efforts to do that is to move that information to the patient. So patients do have the right to get access to their own health information, and the federal government has undertaken a number of initiatives to encourage them to do that. One of those is under the incentive payments for doctors and hospitals under the Affordable Care Act to adopt electronic health records.

One of the key functions that they need to undertake is to allow patients to view, download, and transmit their own health information. But what happens then is we have, and we are encouraging people actively to move their information potentially out of the HIPAA covered bubble and into the hands of others who may not be subjected to HIPAA.

Having said that, there are circumstances, for example, when you have a personal health record that is offered on behalf of a health plan or a health care provider. Because they're so tied to the plan and the provider, that information would remain protected within HIPAA.

If you transmit your information-- you know, you're a patient and you're looking on the website you just find your own personal health record website and you say, hey, I want my information sent there, then it wouldn't be protected. So you can see how it's a little complicated.

CORA HAN: Thank, Joy.

JOY PRITTS: Thank you.

CORA HAN: So turning now to some of the other products and services, like websites, apps, and devices that increasingly put medical tools and health data in consumer's hands, what are some of those products and what are their benefits. And Sally we might start with you.

SALLY OKUN: Sure. Well, thank you very much.

There's just such array of them, and we heard a little bit about that in Jared's talk in terms of the kinds of apps and other devices, sensor devices, that are available to people today. So I think I won't spend a lot of time there because I think he gave us a really nice overview of that.

But I think where we need to be starting to think about is first of all, the habits that people, as consumers, already have in using the internet looking for information about their health. We know that nearly 75% of adults in the United States are already online looking for information, and many of those, about 60% of those are actually looking for health information.

So there's a variety of things that they are going to find there that could have varying degrees of usefulness, utility, as well as privacy protection. So one of the things that I think is important is for us to all think about how we practice on the internet and where are we going, and that will help us to understand, I think, sometimes the kinds of things that are available.

So there's a variety of things. We have access to websites that are particularly focused on a particular disease, so you'll have a lot of websites maybe dedicated diabetes, where a lot of information can be pulled in from an app, for example, or a mobile device, and it could actually create a profile about you, individually.

There's others that are really more around support. And I'm thinking about well, I have this condition and you have this condition. Let's try to find ways of being able to share what we know and then find some ways of supporting each other.

And then there are apps like PatientsLikeMe, which I'll give you just a brief overview of that, is really more of a research-based concept on our platform where we actually are helping patients create health profiles using quantified survey type tools where they're able to create information, and then longitudinally track that over time.

It happens to be built upon a social network. So the concept being that patients actually have the opportunity not only to create their own personal record, but also to share that and be transparent about that with other people like themselves.

I think the other piece that I want to mention about PHR, as in Personal Health Records, is one area that has not necessarily taken off, is the fact that personal health records are actually rather boring. Really, there's a lot of things you can do there in terms of transactional things, like make a doctor's appointment or maybe check your labs, pull in some information whether you're going to view down and transmit that information. But there's not a lot else to do.

So I think consumers, in general, are looking for something a bit more interactive, a bit more informative, a bit more ubiquitous in terms of being able to bring in other information about themselves in a meaningful way and then make some sense of that, with others, oftentimes like themselves.

So there's a whole host of ways of being able to find users on the internet to start answering questions that you might have, either about your health, the health of others in your family or loved ones that you care about. But the variety of them are so diverse that you really have to start thinking about what's the purpose that I want to use it for, and then understand what your risk might be in using it for that particular purpose.

CORA HAN: Thank you. And Joe, did you anything to add? I know you've done some research.

JOE LORENZO HALL: So that's a wonderful overview. There are a few things that-- there's just a zoo of health and medical apps, devices, and websites out there. There are a couple that haven't been mentioned yet.

So, for example, your phone often can integrate with things that provide some aspect of medical measurement. And so there are simple things like wireless scales that can upload your weight to a PHR or some other service.

We have wearables-- there's one in the front row. I'm not going to point to the person wearing it. But there's a lot of-- oh, she's laughing. She outed herself. But there's a lot of sort of recording your daily habits so that you can keep track of your health and wellness. In some cases these may be maybe not prescribed by a physician, but at least at the moment recommended heavily by a physician.

And you have sort of the vanguard of integration of sort of health wellness and medical tools. So there are, for medicine reminders you have things like a pill you take every day that actually has a little microchip in it that interfaces with your smartphone to make sure that if you have mental problems that may cause you to forget to take your medication, it will actually assist you in doing that.

And finally, there are really innovative things that we don't really know what to do about yet. For example, Google announced project IRIS, which is a smart contact lens that will measure-- hopes to measure, I guess they would say, your blood glucose level by measuring that quantity in your tears. And you put your Android device close to your head and it would let you know, oh jeez, you probably need to take some insulin or something like that.

So there's a real zoo, and I'll be brief so we've got plenty to get to.

CORA HAN: Thank you, Joe. And Chris, we know your company has a great product that we would like to give you the opportunity to talk about. So if we can see a personal health record in action, that would be great. So if you can give your demonstration now.

CHRISTOPHER BURROW: OK, Thanks.

Well, let me start by saying thank you to Kristen and Cora. And I'm delighted to find that the Commissioner is here, and wonderful to meet you, Commissioner.

So couldn't ask for a better set up. HIPAA's been explained, but I chose that as my first slide. And I want to highlight what Joy said, which is that with HIPAA, we, as citizens, all have a right to our health care data. And with the updated version of HIPAA that you heard about in the HITECH Act, we all have a right to electronic data.

And I like this memorandum that Leon Rodriguez has prepared, who is the Director of the Office of Civil Rights. So that any citizen who goes to his health care provider or hospital can take this memo, and it really details exactly what my rights are as a citizen, and so there.

But one important thing in that memorandum is that it draws attention to the fact that with new electronic health record systems and personal health record systems, patients can now help. They can now help to keep themselves safer, and to make medical care better.

And so this is a very positive development, and we're at the dawn of tools being offered to patients that can have them do just that. So what I will hit very quickly is the description of the iBlueButton app, which Humetrix started building about four years ago.

And this is a native app that runs either on Android or iOS devices that allows you to take care of yourself and your family members by collecting health records either from places like Medicare or the VA or TRICARE, or even now, from hospitals and doctors offices that have EMR systems.

And as you can see here, this particular patient-- I think I have a pointer-- this particular patient has several records. This patient has a Medicare record, has a record that he's obtained from TRICARE, which TRICARE online is the online site where active duty soldiers and their families can go get a online Blue Button record or their summary record.

As well, this particular fictional patient has acquired data from an EMR system called Epic at University of California-San Diego. And all of these records are captured in the app where they're stored locally on the device. And the system allows you to create a summary record, that is, your medications, immunizations, allergies, and conditions that are abstracted from all of those records.

Now, there are several ways to get data into this app. And by the way, all the data is stored locally on the device. There is no silo. There is no cloud. Everything is local on the device where the data is kept safely encrypted.

Any document that you might have on your desktop you can upload into our app. Or you can use the camera function in the app. If you've burned your hand, to take a picture of the burn every day and you might want to share that with your physician when you see them, or if you have other skin lesions so that they can follow the course of what's happened.

Now, this is a summary of the features of the system that we've created. And so on your left you see the version of the app running just here on a-- sorry, going backwards-- running on an Android device, but also on an Apple device where the user can download records from Medicare, VA or TRICARE.

What kind of records are those? They're called a Blue Button record. You might see on my lapel I have a Blue Button. This is a federal initiative that Joy was commenting about, where the federal government, led by the Office of National Coordinator for Health Care IT has gotten together with a group and developed standards that allow individuals to safely, securely receive that data in a defined format for their benefit.

Now, Medicare, along with the VA led the way. And any one of you, if you're covered by Medicare or family members are covered by Medicare, can go to mymedicare.gov website, go through an authentication process there, acquire your login credentials, and then enter those into the app where they are stored on your phone. And you can download the record, and the app will present it in a very user-friendly format, shown there, where you can see the record.

And also, most importantly, what I didn't say in the last slide is you can push that record over to your doctor's iPad with a secure device-to-device data transfer. Again, no data residing or persisting online. Where the physician can see your data, plus any annotations that you've made.

So we're giving you a secure way to receive your records, store your record, and share your record. And I just might say in passing that 37 million Americans who are covered by Medicare can use this technology today to receive critical information about all the medications that they received in the last three years have been paid for through Part B. As well as all conditions that will have been coded for them by all physicians.

Now, just to step back and let me tell you why I'm passionate about this. There are in this country somewhere between 100,000 and 400,000 deaths due to medical errors every year. There are at least 700,000 adverse drug events that result in injury or death.

Just having your mom's medication record available to her when she sees her doctor, or you, yourself, having your own goes a long way to preventing adverse drug reactions. This really can be critical, crucial information, and we're passionate about delivering this service to our users.

The new way to get data, you've heard about downloading data from the Medicare Blue Button or VA, the new standards have been put in place called the Blue Button+ standards require that hospital information systems use something called Direct, which is a secure email protocol to send a defined machine and human readable summary of your encounter or your hospital discharge to you, to a email address.

Our app provides you with that secure address. And the physician or physician extender or nurse practitioner can send the record directly to your app. Our app will download it, let you view it, and let you assimilate it with other records that you have to create that summary record.

Here is an example. There is the Medicare record on the left, showing all the diagnoses and all the medications, and you could scroll down and see your visits and imaging studies.

The next record is an Epic EMR system record from University of California-San Diego, just to show you, you can view it. The next record is from the VA. And then the last display over there, the summary record, is what I was telling you about, where the app has now gone and retrieved, if you will, by parsing through all the data and the other records, all of the medications that you've received, as well as all your conditions.

Just to finish up here, and quickly, because I think this is quite important. If we look at both medications and conditions, you can have a detailed view of your medication. You can tap this great resource from the National Library of Medicine called MedlinePlus, and instantly see side effect information about your medication.

For your conditions, you can easily see information about your conditions in English or in Spanish. And our app lets you indicate whether or not for a drug you're actually taking it or not, whether you're having any side effects or not, and would you like to keep this entry private.

And the same thing for your conditions. There are frequent errors in medical records. Our app lets you indicate if a particular condition is error, or whether it was in the past, or whether or not you would like to keep it private.

So the way our system works, when you share that data with your physician, if you're sharing the summary record, the only thing that they will see is the items, item by item, that you've decided you want to share.

Were you to share the entire Medicare record or the entire record from the VA, that record goes across unaltered. So you, the consumer, are in control with this app.

So one thing I'd like to finish on is the privacy policy. So within the app there is a privacy policy. And you can see we also have an About statement and a FAQ statement that explains how to use the app. And if you tap on here in the privacy notice, you can see the ONC's model privacy notice that we've put into the app, so you can see it right away. And this shows you whether or not we release any of your data.

Well, first of all, since we don't have your data, we cannot release it. So no, we don't release it. Do we require any limiting agreements? Again, not applicable. And with regard to any particular details, we essentially don't release anything.

So if we go back to the data map-- I love the data map that Latanya Sweeney showed at the start-- if we go back to the data map, this is a new kind of PHR. Here, PHR is essentially irrevocably tethered to you and only to you. You're not sending your data somewhere else out on the galaxy

of all those places where there's a new data silo about you. Should you care to or choose to, you, of course, have a right to, but using this app you don't have to.

So with that, I'd like to conclude. And Kristen, and Cora and everybody, thanks so much for giving us a chance to speak.

CORA HAN: Great. Thanks, Chris.

[APPLAUSE]

So turning from the marketplace to privacy concerns, we spent some time this morning talking about data flows. And certainly, one of the most significant privacy concerns we've heard about is the potential for sensitive health information to be shared in ways consumers would not reasonably expect or anticipate. So we'd like to spend a little bit of time talking about these flows.

And I think we'd like to ask the panel, and perhaps, Joe, you could start off and then others could jump in. Can you tell us about the types of data sharing you've seen in the app world, as well as PRHs and elsewhere? And what sorts of business models are in that space?

JOE LORENZO HALL: OK. So you want me to specifically talk about business models first or talk about-- there's sort of two pieces to your question.

CORA HAN: How about we start with the sharing and then we'll--

JOE LORENZO HALL: OK, sharing.

CORA HAN: --move on to the business model.

JOE LORENZO HALL: So as Latanya's map sort of showed, there's quite a bit of sharing in the traditional sort of more clinical medical services delivery health care industry context. We don't know a whole lot about the sharing of apps, other than what we've seen from the Privacy Rights Clearinghouse study, the Abingdon study. And now the FTC's adding to that set of results.

But there's other research. So for example, Heather Patterson, who couldn't be here with us today, has done a really interesting, fascinating, deep qualitative study of Fitbit users. And if you don't like qualitative methods, well, you're missing out and you may not like this work. But talk to me later. I have a degree in astrophysics so I can tell you why they matter.

But anyway, the top concerns from people that they started using Fitbit, which is, I mean, that's pretty benign information. It's sort of to some extent how many steps you've walked from an altimeter sense, and then your actual motions translated into how far you've walked.

But the things that people cared about were, the top three were sort of embarrassment, physical safety, and then implications for employment and insurability. And so in terms of embarrassment, Fitbit has a great case study itself where they were accidentally sharing

individual's sexual activity publicly online, without them knowing, because you don't typically wear your Fitbit when you're engaging in that kind of activity.

But you can self-report that kind of activity. And if you're sharing everything, you're sharing that as well.

That was very embarrassing to those users, and Fitbit very quickly, to their credit, recognized that some categories of physical exertion may be a little more sensitive than others.

[LAUGHTER]

I didn't even intend that to be a joke. That's awesome.

But physical safety is another thing. So if you talk about routes, running routes and things like that, you may able to predict where someone is alone or when they're not at home, and that can be extremely sensitive, given your own personal context.

And finally, employability and insurance rating. We've talked a little bit about insurance rating, but to some extent, these kinds of devices or these kinds of patient generated, or consumer generated, I guess I should say, health data are increasingly being used in wellness programs to reward people or to encourage them to be more healthy, if not just for the bottom line given your health insurance premiums. Other things as well, in terms of making it a better working environment.

There's other things, but I won't talk about them. But certainly in the business model side, and this is something that Chris may be able to enlighten us a little bit about too, since he rolls with a lot of people who work with health apps.

It's unclear to me the monetization sort of models are not very different from health apps from other kinds of mobile apps at all. So for example, there are things that are just purely ad supported, and clearly the top 12 free ones that we've seen are those kinds of things. There are freemium apps, so this is where you get something for free, but if you want some extra service like knowing exactly what that drug does or something like that, you may have to pay a little bit more.

There are sort of one time payment. You pay for an app and then you never have to pay again. And there are subscription apps. There are ones that feel that they provide such a service and people pay for these things, that on a monthly basis you pay some money for that kind of stuff.

And the ones that definitely seem to engage in a whole lot of sharing tend to be the ad supported model ones where you have somewhere like an average of 15 different services receiving various kinds of details about the user.

CORA HAN: Thanks.

CHRISTOPHER BURROW: Sure.

So with regard to the BlueButton app, we have a freemium model. So for the consumer, the consumer, any one of you, can go on iTunes to Google Play Store and download the iBlueButton app, and it's a free download.

Currently, since that version of the app that I just showed all of you-- it's brand new. We just released it at this year's HIMSS Conference-- were on special. It's absolutely free now. But coming soon we will have the equivalent of a subscription model.

Again, we believe that the client who pays for the app is, in fact, the client. If you're not paying for something, you're probably not the client. So we believe there is real value in letting people have access to this kind of tool where there's absolutely no data sharing outside of the confines of your device. So that's how we market this directly to consumers.

JOY PRITTS: Cora, I'd like to jump in and say I think one of the areas that's kind of interesting is that people might say I'm willing to give you my information to get this product for free. And they might not realize what some people or some organizations do with the information after they receive it.

So there is a certain amount of lack of transparency, and going back to the data mapping, of what happens with the information after it is collected by the first third-party. Because many of those third parties actually go ahead and they resell the data to other entities. And sometimes that information is anonymized or pseudonymized, so that it might not necessarily have the individual's name attached to it.

But some of the value in the information is actually being able to associate that information from that device with information that's collected from other services, such as your CVS card-- your frequent flier card from Giant or Safeway or CVS, or somebody like that. Or even your frequent flyer miles.

And there are data aggregators that are in the business of collecting this information, not from what we consider your health, your core health people who are in organizations that are covered by HIPAA, but by these other kind of outside players in the market now. Where people probably don't have a good idea that that's happening with their information.

CORA HAN: Thanks. And so de-identification is definitely an excellent issue to bring up, and we will be circling back to it a little bit later today.

But I had another question I wanted to sort of follow-up here with, and that's to any of you here today, are you aware of self-regulatory efforts limiting the use of health data for online marketing purposes? What sorts of things have you been seeing?

JOE LORENZO HALL: So I can certainly talk about that.

There are a smattering of self-regulatory guidelines and codes and principles. The AMA, the American Medical Association, and the American Medical Informatics Association have some

guidelines for electronic communication with patients. Now that's very different than consumer-- it's very narrow compared to consumer generated data.

The Department of Commerce has something that touches on this, which is the NTIA Mobile App Transparency Code of Conduct. And I know there's people in the room that have been there with me hammering that out. And it actually requires very clear short form disclosure trying to get at the transparency issues for collections of biometrics and health medical and/or therapy information.

And finally, the Digital Advertising Alliance and the Network Advertising Initiative, the two main advertising guideline bodies, I guess is the way to say it, have mobile behavioral advertising guidelines that apply to sensitive health information require explicit consent before some kinds of uses, like behavioral require the user to give explicit consent before they can do things like behavioral advertising.

But there's nothing that's sort of more gen-- that I know and I'd love to be proven wrong-- that's sort of more generic, that is sort of guidelines for health apps that may or may not be using sensitive data. And I'd love to be corrected, but it's the kind of thing that I think the time has come.

CORA HAN: Thanks. Anyone else have anything to add?

SALLY OKUN: I would just add that consumers themselves, when they're starting to use some of the features that might be available to them. For our site, for example, I think Latanya had mentioned transparency establishes trust.

And one of the things we recognized early on in creating PatientsLikeMe was that we needed to establish the trust of the patients who were going to be using the site in such a way that we held that as one of our highest core values. Without it, we really won't have a site.

So we pay a lot of attention to our user agreement, to our transparency and openness policies that are very prominently displayed. To let people know, first of all, that their data will be used.

We actually aggregate, de-identify, and then make that data available to interested parties. That might be pharmaceutical companies, it could be government, it could be clinical researchers who want to learn from the experience of people living with chronic illness over time. So we're very up front about that, and I think that that's something that's critically important.

We also encourage people, in terms of our own guidelines, not to use their real names, to be careful about the kind of information they're sharing within the forum conversations. But also to recognize that it's their choice.

So we will oftentimes see people with real pictures on the site, and it's not necessarily something we would promote. But we also recognize that that's a choice that the consumer themselves has made.

But I think the other piece is in terms of our site, again, I just want to bring that back. One of the things that we've learned is that in terms of the data sharing research that we've done is that for the most part people are really willing and interested in sharing their data for a couple of really important reasons.

One is they want to know, in our experience anyway, is my experience normal. They'd like to be able to share with other people like themselves to better understand whether or not what their experience seems to be what other people like them might be experiencing.

One example is in epilepsy, we learned early on that about one-third of the people with epilepsy on our site had never talked to or met another person with epilepsy before. And it's a very stigmatizing condition.

The second most popular reason that they give is altruism. I want to have my experience benefit other people. So I think we need to find a way of unpacking some of the ways that we can make it easier for patients to share this kind of information, without necessarily compromising their privacy to degree possible, recognizing that when you're on the internet your privacy is subject to being revealed. And that's not something any of us can fully protect.

But when consumers are aware of that in the most explicit and transparent way, I think we actually elevate their willingness and their appreciation of why sharing health data can be actually quite beneficial, not only for them, but for others like them.

JOE LORENZO HALL: I forgot to mention one thing that my employers would be mad about.

So at CDT we're also working on big data and health, and explicitly looking at the Fair Information Practices and to what extent they need to be tweaked, because we don't believe they're relevant any more.

So that's an ongoing project that's going to take a good chunk of the rest of this year, but myself and Justin Brookman, the Director of our Consumer Privacy Products, and Gautam Hans, our Plesser Fellow in the back are working on this and if you're interested, let us know.

CORA HAN: Thanks.

KRISTEN ANDERSON: Thank you.

Joy, there was one other aspect of unexpected data flows that we wanted to ask you about, and that was in the context of electronic health records and the data that can flow from them.

JOY PRITTS: Well, everybody receives a HIPAA privacy notice. How many of you have ever read them? So people here have. Most of the time when you ask-- I will also tell you that we have, in the course of work where we've done-- not at ONC, but in my past life where we did focus groups.

There is information in those notices that people just don't read. There has been a revised version out that puts patients' rights out first, instead of the uses and disclosures to try to highlight some of those uses.

But one of the uses of information that many people are surprised about is their use of health information for research. And there are ways that health information can flow for research purposes that happen without the individual's expressed permission. And that surprises a lot of people. It's totally legal, but it's surprising.

I think one of the ways that the research community is headed is very important for us as we move forward, which is patient-centered outcomes research. And that's really looking to not only clinical trials, but looking at a person longitudinally to see not only how they're treated, but how they're living and what activities they're undertaking.

And after they've been cared, how did that care work? And how were those health outcomes affected?

There are some organizations that have formed their independent third-party organizations to really undertake this research. And they have found that it's really valuable for them to collect the information, not only from the health care entities, but also from things like, we mentioned a little bit earlier, your Safeway card. Your frequent flier card. Your purchase data. Your financial data.

Because there are often correlations in other types of data that when matched with their health data, they believe may prove very informative about predicting what will work and what will not work with people in terms of treatment. So it's something that I think a lot of people find a little bit surprising, how all of those little nodes on Latanya's map can also actually be brought together.

CORA HAN: Thanks.

So building upon something you touched upon, let's pivot a little bit and think about consumer perceptions of these data flows. And perhaps, Sally, I'll address this next question to you.

You were recently involved in an Institute of Medicine study regarding social networking sites and continuously learning health systems, which reached some interesting conclusions about social media users and the sharing of their health information, and what type of sharing they're comfortable with, and what type of sharing they may be less comfortable with. Could you comment a little bit about that?

SALLY OKUN: Sure. The study was actually done as a follow-up study to one that was done by Consumer Reports that actually had just a couple of questions in it that related to health data sharing that piqued our interest at PatientsLikeMe. And the question had to do with would you be willing to share your health data if it were to improve your care or the care of other people like you? And nearly 90% of a nationally representative sample within the country agreed that they would be willing to do that.

Now, when asked whether or not they thought it was happening, most people either didn't know or said no. So there's sort of a sense that I'd be willing to do this, but I'm not sure if it's being done, and if it is being done, then maybe I need to know more about how that works. And I think that speaks to Joy.

So we actually learned quite a bit. What we decided to do was take that question and then expand upon it within our population of chronically ill people. So we actually were able to sort of tease out a little bit. We know the patients on PatientsLikeMe are already sharing their data. So it wasn't surprising to learn that 98% of them were willing to share their data, if it was going to benefit themselves or someone else.

But what we wanted to find out also was who were they willing to share that with outside of PatientsLikeMe, Like Me and were they already doing that. And also, what were their concerns. And so we did learn a little bit more about what makes someone hesitant to share data outside of the walled environment of PatientsLikeMe.

Certainly, we've heard some already. 76% of the patients interviewed thought that their data could be used without their knowledge. So we already know that it is being used without their knowledge. It's moving on to different places. So that actually validates that concern.

72% were concerned about their benefits and being denied benefits. Now, whether we re-ask that question today in the light of more health coverage, that might be an interesting finding. This was about two years ago that we did the survey.

And then 66% really were worried about limiting job opportunities. So there's real clear reasons why people would be a little reticent to consider having their payer learn a lot more about their health data. Whether or not their employer, again, tied oftentimes to payers, might be learning about this information.

So those are things I think we need to be sensitive to. But when we started asking outside of PatientsLikeMe Like Me who are you already sharing some of this information with, we were actually surprised at how little people were sharing.

So given an environment where they felt safe to do this, they were ubiquitously sharing. But when we asked how many were sharing it with their spouse or a significant other, only about 30% actually said that they actually share the information on their profile with them. And it went down from there.

So their health care provider, 19% said they were sharing it with them. Now, we found that interesting because-- and we haven't teased it out, and Chris and I were talking about this before-- we know that some of our patients are bringing their data to their clinicians only to be rejected, to have them say I don't know what to do with this information. So I'm not so sure, let's not even go there.

Some of the conditions, when we looked at more specifically where that kind of information is being used at the point of care, is in the mood conditions and psychiatric conditions where therapists and patients are using this data quite effectively to monitor moods and things like that.

Another patient outside of PatientsLikeMe, about 16% were willing to share with other patients. So again, when you start to get out of this environment where they felt a sense of trust, they were a little bit less sure that they want to. And their children, only 9% felt that they wanted to share this information with their children.

Now, not out of this study, but another survey that we had done a couple of years ago, we also asked what kind of information are you not sharing with your health care provider. And it was really quite not surprising, actually, to learn that they weren't sharing things about their sexual dysfunction or sexual health. They weren't sharing things about behavioral things, like drinking and that sort of-- and not being quiet as honest about their diet.

However, when asked are you sharing the same information with your peers on PatientsLikeMe, almost 100% would say I'm more comfortable sharing it here. It's anonymous. I feel like I can share that and be honest about it. And people can respond to me in a way that I can actually appreciate and then respond myself, behaviorally.

So it was really interesting to start seeing out we share some things with some people because we're going to get some sort of reaction possibly or not. And then with others because we might get some benefit back by sharing that that might actually help us be able to deal with whatever it was that we were sharing that with.

CORA HAN: Chris?

CHRISTOPHER BURROW: Yes. I'll just make an extra comment.

So one thing that we're finding is, and this is because some of our users call us up. We have actually no way of knowing anything about our users. I don't know any of their names. I don't know anything about them. They have all their own data.

But people do call us up, and one thing that we're being told is that with regard to physicians, we're now putting in the hands of patients, a full medical data set. So let's take drugs. Brand name, molecular name, dosage type, dosage form, NDC code, every single date where it was ever filled, you have on your app. You can share that with your physician. This is hard data.

And anecdotally, what I like to say is, and I've had patients tell me this, it's so infuriating, when I go see my doctor now, he looks at his computer screen and he never looks at me, and he types and everything.

And suddenly I have something on my screen and he'll have to turn around and look. It's like look at my screen. Because now, suddenly, we're at the dawn of this new age and that's what we're passionate about, of giving consumers the actual wherewithal technologically to have a complete or as complete a data set as possible today.

So that's suddenly putting consumers in a much more powerful position to help their physician take better care of them. So this is the start of something new and very, very important. Technology, very sophisticated, in the hands of patients that they can use to be helping with the health care system, instead of just being passive recipients of health care.

SALLY OKUN: Can I just follow up on one topic there?

CORA HAN: Sure.

SALLY OKUN: And I think it came up before.

One of the things that Patient-Centered Outcomes Research is doing is sort of suggesting that we actually start making good use of routinely collected data at the point of care. And we're not necessarily doing that well, in terms of quality improvement and continuous learning.

So this is something that, as consumers, we can be teaching people that it's really important for you to understand that as we collect routine data at the point of care, we're going to start trying to make use of that so we can start to understand things from a comparative effectiveness perspective and that sort of thing.

What we also now need to start doing is have policy and clinicians catch up with patient generated data, consumer generated data to say this is value at the point of care. It has a unique perspective we previously have not collected. And we have to find ways of being able to expect that that data will be respected and honored at the point of care. While the same time not overloading clinicians so that it doesn't fit into their workflow.

So we, as app developers, or website owners, and then people who are working from this perspective, have to understand that the clinicians need to receive this data in formats that they can make use of it and not feel that they're overwhelmed by it. So that we have a balancing going on there.

Thank you.

CORA HAN: Thanks. Joe--

JOE LORENZO HALL: So I'm going to put my Heather Patterson hat on. So Heather and working as a post-doc with Helen Nissenbaum at NYU has done a study of Fitbit users. And part of what they were trying to figure out is what do Fitbit users think they know about what Fitbit is doing. What are their concerns about the possible future of Fitbit's business model.

And I'm sorry I have talk so much about a brand, but it's because the study's about a specific user community around a specific brand. And then what kind of data management practices to people employ to manage that kind of uncertainty.

The one thing that is interesting is people have no clue how Fitbit is a business. Is it selling the device? Is it doing other things with data? They just don't know. And to manage that uncertainly they employ a whole bunch of really interesting tactics.

For example, people don't sign up without using their real name because it's hard for people to-- it's a social challenge, I walk farther than you kind of a thing. So there's an important role having your real name involved with that.

But people will only share with folks that they've met in real life, often. Or they'll only share with people they've never met, because they don't want anyone knowing about their regular daily habits. And so there's a sort of really interesting social divide with how people are using these kinds of tools.

And the fascinating thing is that people are thinking a lot about how Fitbit's, specifically, business model might change. And so they don't know what may happen in the future. And in some cases, you see worries about things like who has access to the data? Who potentially has access to the data? Does the government have access to this data? Under what circumstances can-- if there's a fist fight in a bar, can the accelerometer data be subpoenaed off of my Fitbit to prove things about whatever.

So there's a whole bunch of interesting sort of social management practices that are sort of appearing and evolving with the uses of the more wellness devices. And I think we'll see those, too, with health, and with specific medical interactions.

CORA HAN: Thanks.

KRISTEN ANDERSON: Thanks.

So one of the other significant privacy issues that we've heard a lot about is transparency, specifically via notice and choice. What are some of the challenges providing effective notice, and what are some of the ways of meeting those challenges? For example, we hear a lot about information asymmetries resulting from poorly crafted or very long privacy policies.

Joe, would you like to kick us off?

JOE LORENZO HALL: Sure.

So it's often said that notice and choice is-- that notice and consent is dead. We at CDT don't believe that. And what people tend to say when they say those things are, no one reads privacy policies. And that's so true except for a few of us who for some reason get a kick out of it, right?

I guess there are people, that it's part of our job, we have to read these things and that's a good thing. But at the same time, if you're expecting people to read 30 pages of legalese and understand it and be fully informed, you're going to have a bad time actually communicating with people about what you're doing. But that's why there's a bunch of other efforts.

So, for example, there are some platforms, like Apple's iOS platform that use Just-In-Time notifications. So this app is trying to access your location data, yea or nay. And if you say nay, then it's not going to get that. If that's a mapping app, that app may have very little functionality after you deny where you are. It may just not be able to do things like directions and stuff like that.

There's also, as I mentioned earlier, an effort at the NTIA, the Mobile App Transparency Code of Conduct, that focuses on short notice, and there's a whole lot of academic research that is evolving and tends to be sort of on the short notice. Even short notice is very hard to communicate effectively with people.

But I like to think that the NTIA process which shows here's the data that's collected about you using this app. Here are the entities with which the app shares this data, on one screen or a couple of screens of easy, popping sort of interactivity.

I'd like to think that that will evolve and be something that people tend to recognize. Sort of like a nutrition label. It's something you know where it is, unless it's something that's too small to have a nutrition label on it, you can find it. You sort of know how to interact with those kinds of things.

In the longer term, I do think that it would be neat to have Just-In-Time notification for storing and access health data. So if we could get mobile platforms to actually carve out a little chunk of its operating system to store things like a CCD, a Common Care-- I forget what the acronym stands for-- a summary of your clinical interaction.

And then the app could say this app was trying to access your medical records. It was trying to store something of a health data nature to you, and if those guidelines were enforced by app stores, that could be a really neat thing and to allow people to have some of the things that Humetrix and iBlueButton do in this very controlled sort of environment. But make that available on a more platform, a more generic way.

CHRISTOPHER BURROW: Well, certainly we started four years ago to build an app that was highly secure, all native, you control your own data. We also built in privacy warnings.

For example, even though the data transfer to the provider's iPad is completely secure, uses a time cryptographic key, is resistant to all man and metal attack. There's no data persistence. We still put up a little warning saying, you're about to send your health data to this person with an iPad. Be sure it's the right physician. And you both authenticate each other and look at each other. So we think that's great.

With regard to the ONC's model privacy notice, we think that's a step in the right direction, which I'll refer to as the soup can label idea. I'm not sure that people really read soup cans that much, Joe.

JOE LORENZO HALL: I do because I'm hypertensive. So--

CHRISTOPHER BURROW: But that's a great idea. And so there are nos and yeses that are pretty clear there. I think there needs to be those kinds of simple notices to make it clear.

I might want to set you up again to come back to de-identification because I also read privacy policies. Ours is simple, it's one page. But I've read other privacy policies that say that we'll share data, but it will be de-identified. But they don't specify what that term means. And I'm also a scientist, and so, gee, I wonder what that means. So I think there's a problem with transparency there.

KRISTEN ANDERSON: Right. And we will definitely get more in detail into de-identification in just a bit. But I think there's a second component to the transparency and notice and choice thing, and that is about contextual use of information. So you might have a soup label type notice up front, but then back end use. And we've heard a little bit about that in the presentations, and some of you have mentioned that as well.

So what about when data about patients is linked or re-purposed after the fact? So it might be covered in the privacy policy, but then used after the fact. How do you work to provide effective notice and choice around that?

SALLY OKUN: I can speak to PatientsLikeMe. I mean we, actually in our privacy policy, transparency and openness statements are pretty clear that the data that you are going to be providing will be and can be used for aggregation, de-identification, and then shared with our partners, whomever it is that we're working on a project with.

So that's the basic profile data. That said, when we are actually in the process of working on a particular project or we're doing an initiative or a survey study, that reminder comes in as part of the consenting to participate in that survey.

So that information would clearly tell them who our partner is. It would clearly tell them how that data is going to be used in the context of this new survey or this study that we're working on. And we also promise then to give that data, the findings from that data, back to them within a reasonable period of time. That's a promise we make with almost everything that we do. It's sort of give something, get something mantra that we have.

So every time you give us a piece of data, we either give you a graphic display of what that data means in the context of everyone else on the site. Or when we're doing a specific study that's targeting a particular set of questions, we will bring that data back to the users either in a blog post or in a form or in some format for them to be able to know here's what you contributed, here's what the findings were, and then generate some conversation about that.

KRISTEN ANDERSON: So we've also heard about privacy being a share responsibility. We've heard a little bit from Sally and others about that. And we just wanted to follow-up a little bit on what consumers should be doing. If they only have control over, say, entering the information once into the app that they're interfacing with right then, and then it goes on to be shared in the back end, how can they keep their data in the context that they would expect?

JOE LORENZO HALL: So it's a double-edged sword with no handles, so to speak. Well, maybe that's not right. The double-edged sword of view, download, transmit. View, download, transmit is awesome. People have their data in their hands. They can do a bunch of stuff with it.

The double-edged sword part of this is that people can do really silly stuff with their own data now, and they can do things that are sort of irresponsible. But that's part of sort of this national negotiation process we're having with increased custody, so to speak, on the patient's side of being able to use and do things with this data.

And so if any of you ever see someone post their medical record on Facebook, that's a really good opportunity to have a conversation with that person about what's appropriate, and how that might not exactly be the thing that you'd want to read, being an audience member for that person's Facebook profile.

But I think there's a whole set of social practices in terms of people that are thinking about things that are more knowledgeable about these things should really keep your eyes out for that kind of stuff.

But consumers in general are going to need to think harder about these things. There are going to be some fantastic mistakes that happen that will serve for folks like us, who are consumer advocates can go out and say look, don't end up like this. Please protect your information more like that.

On the NSA/Snowden side, we're doing a whole lot of stuff with making sure that people can properly protect their data, be it a communications session, or data at rest-- stuff you have on your computer or your mobile devices.

And so I think there's larger trends of everyone needs to sort of bone up on their digital hygiene, so to speak, and understand things like password managers. I have 1,200 passwords, I only know two of them. You should never have to know more than that, because there's really good tools that will help you create secure ones and you'll never have to remember another one again.

There's a whole slew of sort of things like that that as a society we're going to learn to incorporate into the sort of fabric of how we do things.

JOY PRITTS: I think that one of the issues that I continuously hear is that there are many people who think, from a consumer perspective, that privacy is dead. Nobody cares anymore. Look, people share all this information on Facebook. They engage in this behavior in social networks, so they don't really care.

I think there are also are a lot of research studies that have come out within the last year or so that really question that perspective. Because people who have had something happen to them or know something that's happened to somebody due to the information that was posted on their website or something of that nature, have a renewed respect for their own privacy and how their information may be used.

I also think that people, there's a segment of people who care a lot about privacy, and there are people who would share everything with anybody. Again, sometimes those perspectives change when you realize what the consequences of that sharing might be.

And I also think that when you hear this conversation, its like well, only 10% of the people in America really care about privacy. But that 10% or 20% is flexible. It's not a static number.

People come and they flow into and out of how much and whether they care about how they're sharing their information, depending on, again, on the context. So I think there are a lot of nuances to the discussion about first of all, people's perspectives on privacy, and what they're willing to do to protect it.

Some people have a lot more at risk than others do, and that changes over time. It's a very dynamic issue.

KRISTEN ANDERSON: Did anybody else have anything to add to that point?

SALLY OKUN: I would just add I think that all of this is so true. We are entering a time when consumers are going to be expected to have a lot more ownership of their own health and their health care. And whether you want that responsibility or not, it's coming your way.

So I think there's a lot on all of our parts to be able to start thinking about what is it that I need to know? Who do I need to learn it from? And where might I get this information to start protecting myself?

I think it's just very clear that we probably can't protect ourselves from a lot of this third-party push that's going on, because first of all, we may not even be aware of it. But when we do become aware of it, we begin to have an increased sensitivity, I think as Joy's already said.

But I also want to reinforce that even people with chronic illness who are participating in data sharing significantly on PatientsLikeMe have an expectation that we protect their data. They have an expectation that we anonymize that data, and that we can de-identify that data.

That expectation is something that, again, as I said earlier, were we to violate, we would be not able to have the trust of our patients. So I think there is an expectation, especially among those who feel that they have a lot to lose if some of that information were to become available outside of the sphere that they expected it to be used in.

But at the same time, each of us, I think, as consumers are going to need to expand our awareness and understanding. What can we do personally, since we will be given a lot more responsibility to have our access to our medical information that we previously have not had available to us. As well as, begin to share that in places that maybe are not as protected as we might think they are.

CHRISTOPHER BURROW: I'd also make the point, and the Commissioner made this point earlier today. So we spend a lot of time talking about the cost and the risk of privacy. And those are all very real and we're digging deep.

But the benefit can be extraordinary to having these kinds of technologies available. You don't necessarily have to understand your record. I'm not trying with the iBlueButton app to make all of you physicians or specialists as physicians. But I am trying to give you the basic building blocks, so that that data will be available when you go somewhere else and see another physician.

And so that's really, I think, there is enormous benefit, and I don't want to go, don't have time to go into all the studies that show that just having a medication list that's up-to-date, and a condition list that's up-to-date can avert all sorts of medical misadventures and catastrophes that you, your children, or your parents could be subjected to without this data.

So there's a tremendous benefit, as well as a privacy risk.

JOY PRITTS: And we won't see that benefit unless you protect the data.

CHRISTOPHER BURROW: Yup.

CORA HAN: OK, thanks. So we'd like to move on to de-identification, which has come up a couple of times today. And first there was a question from the audience.

So there's talk-- and then this is what we've been discussing a few times-- about sharing data in de-identified form. So could people comment on Latanya's finding that her group was able to re-identify 43% of the sample? And would consumers appreciate this? And how should policymakers account for consumers not being able to understand?

So there's a lot there, but I--

CHRISTOPHER BURROW: I'll just jump in and make the first obvious comment, although it may not be obvious to a lot of people in the room.

But in the HIPAA guidance on data de-identification, it states very clearly that gender, five-digit zip code, and date of birth-- month, day, and year-- can identify 50% of all Americans. So that's pretty extraordinary.

So there is a real need to have ways of avoiding, putting those three, just those three simple facts together.

JOE LORENZO HALL: I was going to make one slight correction, which is Latanya's original study showed a higher number than that. I think it was 70-something, and then there was a follow-up using the 2000 census data by Philippe Golle, which dropped that down to like 60-something. So it's big.

CORA HAN: Thanks.

JOY PRITTS: I think that there's a large variability in how de-identification is defined.

CORA HAN: Oh, thanks. Yeah. I was going to follow-up with you about this.

JOY PRITTS: Yes. So I think the HIPAA Privacy Rule probably has one of the most stringent definitions of de-identification of any privacy rule that I've ever read.

The paradigm in protecting health information, or any kind of information, is drawn in just every statute regulation I've ever read, and it's limited to identifiable data. And if it's non-identifiable data, depending on how you define it, then the regulation or the statute generally doesn't apply. Because the idea is to protect the individual, not just random data.

So the question then is when does information become identifiable to the point where you can actually attach it to somebody? And that is kind of a moving target. And that has changed, and will continue to change over the years, and as technology advances.

So the HIPAA Privacy Rule has two means under which information can be considered de-identified. One is the Safe Harbor Method where you have to remove many of the elements that Chris mentioned earlier, which are almost all dates.

Zip codes, name-- the obvious ones, your name, your social security number, the medical record number-- to the point where during the comment period when the rule was being written, as some in the audience would attest, that there was a big blow back. Because researchers are saying that we can't possibly use this information because we can't associate it with anybody, and we need to do longitudinal associations.

So as a privacy rule it's kind of tiered. There's also a tier of information of which the major obvious identifiers have been removed. But many of the other information can still be retained, such as dates of service. And that information, there's a recognition that there is some potential there for re-identification, and so that information can be shared particularly if a researcher just goes to research with a data use agreement that the recipient won't re-identify it.

And that is one of the ways that people are addressing this issue is kind of stratifying the information of here's really-- you'll see this on public use sites, and I think NCI did this as well, National Cancer Institute-- here's information where we believe we've done a really good job, and there's some testing done to see how good a job that they've done.

And that information is available in a public use file. And then new information where there is a larger potential of re-identifying the information they make available, but it is subject to some sort of a data use agreement.

Having said that, some of the information that was, for example, the state release of information, is from entities that aren't necessarily subject to the HIPAA Privacy Rule. For example, public

health departments in states-- it's a complicated issue-- but many of those are not covered by HIPAA Privacy Rule.

They are often, though, covered by their own state laws. And how state laws define what kind of information can be shared or how it has to be anonymized or de-identified vary very much. And they, too, are sector specific. So what it says over here in the rule that governs doctors or other health care providers may be different than the equivalent of their Privacy Act.

So de-identification, there's not a single rule of governs everybody.

CORA HAN: And that was actually going to be my follow-up question. So this is something, Chris, you also referred to. There is no standard definition of de-identification sort of across the various products and services.

So here's a question for the panel. Should there be? And if so, do you have thoughts about what it should be?

SALLY OKUN: I'm going to say probably yes, there should be. I'm going to say that there should also be, within the business model of the company, some inherent responsibility for acknowledging the ability to re-identify information that could be used inappropriately. And so I'll speak to that from PatientsLikeMe's perspective.

We are not a regulated entity under HIPAA, however, we adhere to the identification processes of restricted data and protected data, and that's part of our standard operating procedures. So any time, we're working with a partner, they understand that. They understand that the data use agreement that they will sign with us in terms of receiving information will be free of anything that would be considered that.

Now that said, within our environment of working with them in a research project, we will take that into consideration so that that usefulness of that data could actually be considered in the context of whether we want some geocoding kind of information to understand what are we looking at regionally and that sort of thing.

Also, within our own company, we hold each other to different levels of access. So not everyone in the company has access to all of the information. Those of us who are in the process of doing certain research activities or data science activities will have different levels of access. And that's also spelled out quite clearly in our standard operating procedures.

So I think there's a certain level of responsibility that companies do need to rise to, even when you're not a regulated entity. And start thinking about what that responsibility looks like. I'm not one necessarily to say we need more regulation. But possibly we need guidance and policies that can help frame this conversation more so that it's more transparent to consumers.

CORA HAN: Others?

JOE LORENZO HALL: Sure.

So at CDT we're a big fan of the FTC's, the identification-- I don't know if you call it a standard, but it's sort of a rubric or a guideline that I actually forget the first two pieces of it. But it does things like it binds downstream recipients. You have to enter into a contractual relationship to make sure that that downstream recipient doesn't do certain things like try to re-identify stuff.

I don't know-- a standard could be really difficult. It's sort of generic in the sense that being a privacy and security guy and the guy who spent my PhD hacking voting machines, for example. You start to realize that some of these things are case by case kinds of considerations. And in de-identification you want to think about the utility that you want to retain in the data. And you can't really do that in a generic way.

And you also want to think about those threats, the threats to re-identification that might exist, depending on what you're going to do. And if you're going to post stuff online publicly, that you have a severe, a very large sort of threat surface.

So the last point is that, making a sort of global comment, there was a really neat paper issued by something from Europe called the Article 29 Working Party, which was on basically anonymization and techniques for doing an anonymization. So a little stronger than even de-identification.

And they had a whole bunch of really neat sort of like walking you through how to do certain things, like if this is what you want to do with the data, you can shuffle these whole columns and you're not going to ruin the statistical information in there.

But you're not going to be able to-- well, if someone does end up re-identifying that row, they won't really have much confidence in the individual that it was re-identified to because it's a mix of a bunch of people's stuff. But you have to be very careful in how you do that.

So an effort to do a standard may be really interesting. I just wonder if it wouldn't boil down to a few clear cut cases with some more generic case by case kind of guidance. And I do-- I'm also a big fan of the version of the HIPAA de-identification that isn't to remove these 19 or whatever identifying kinds of quantities. But engage with an expert to actually probabilistically determine, given your use, to what extent these might be re-identifiable.

That's a little hard and expensive because you have to engage with an expert and there's not a lot of people who do that. You go try and find more than two or three of them and it gets pretty difficult pretty quick. And we try to do that when people ask us how do we do this well, and it ends up being a few people that are overwhelmed and such.

CHRISTOPHER BURROW: Well, I think we need to get beyond being able to say in a privacy policy, unless you opt in, we won't share. If you do opt in we will share your personal information, but it'll be de-identified.

The next sentence should be we're sharing it-- could be-- we're sharing it with a large, extremely competent, sophisticated data analytics shop that's running big data that will probably be able to re-identify most of your data. That's a different statement. So there's a sentence missing.

The long way of answering this question, I think we do need to move towards more transparency on this issue.

CORA HAN: OK, thanks. So we have another audience question. How do the panelists think we can come to a common definition of what information and when information is health information?

SALLY OKUN: I'm not sure we can. I think everyone-- first of all, from a consumer's perspective, we all value and quantify our health in different ways. So what I value as being part of my health picture may look differently than it does to someone else in the room.

So I think there's probably certain psychosocial kinds of parameters that will apply to health broadly. And then there's physical characteristics and mental characteristics and all that that apply to health broadly. But then when you start thinking about health care, I think you start talking about very specific and different things.

So talking about it from a consumer's perspective and asking them what constitutes their health might look very different than if you're talking to a payer or a clinician as to what constitutes health. And so I think coming up with a common thing that's going to cross cut would be probably pretty challenging.

I think we need to recognize that health means a lot of different things to most of us. And finding ways of being able to understand that and then put that into context I think is probably more important.

CHRISTOPHER BURROW: Certainly there are core things that we all agree are health care data. Names of your medications, the names of your medical conditions, the names of your allergies, the immunizations you've had, the treatments you've had, the surgeries you've had. I mean I think we can all agree on that inner circle. We can agree on a lot.

Now, I agree, as you get larger and larger circles, you start to get disparities in what people think of as health data. So that's where the trouble starts. But to keep it simple, we can also focus on this inner circle of data that we can all agree about, it's health with regard to policy.

SALLY OKUN: The only problem I would suggest with that is that we then lose the nuance of the context of the human element of what health is. So I would say that that would give us a narrow picture, probably a provider or clinician centric picture. And so we just need to be careful about that.

CHRISTOPHER BURROW: It's required, but not sufficient.

JOE LORENZO HALL: And to elucidate that a little bit more, when I was a post doc with Helen Nissenbaum, you may not have known you're pulling from your panel from a similar team, but Heather couldn't make it so now it's just me.

So we did a study of gay males and MSM, men who have sex with men. This is a population that guards their health information very carefully, because it's not something you can tell by just looking at them. And there has to be very specific kinds of circumstances in which they feel comfortable talking about their health information.

The sample we talked to was 30 men of a pretty stratified age group-- very young and very old. And we found extremely surprising things. Like most of these men, while we didn't ask the question it was just clear they were HIV positive or had AIDS.

And that wasn't so much of a big deal, sort of how AIDS is developed now in HIV is developed now in the sense that it's a manageable disease. It's kind of like something that everyone has to know if you're going to interact with folks, even in a non-sexual manner.

But there were things that they found really sensitive that we could never predict. So, for example, one of them was really concerned about his sister who was 25 and still wet the bed.

And that was such a sensitive thing, and their whole family was-- part of the way that they operated was making sure they protected that kind of stuff, and to make sure there was always someone who is sort of indoctrinated into how to manage that condition with her at all times. So if she's out at a bar drinking and passes out, red lights go off and you need to make sure that certain things happen.

But that's not the kind of thing we would have ever predicted. And those were the kinds of things they were really concerned-- because the whole study is about as we go from paper records to electronic medical records, does that affect the ability-- their tendencies to disclose information to their physicians.

And those were the kind of anecdotes they told us about where these things that I had never thought of that we could never sort of encapsulate in a data structure. And that sort of this human element that I think inevitably will evolve as society and culture evolve, and as our health delivery system and the technologies and techniques we use to do that stuff.

JOY PRITTS: I think the recently released White House report on big data makes a very good point when it points out that what is health data and what's financial data and then other types of data is really merging. And as we accrue this data and collate it and use it, it is going to be harder and harder to draw that line of what's health and what isn't.

I think that people's spending patterns, for an example would never occur to you would be your health data. Yet that information may be used at some point you treat you. And then it does become your health information, doesn't it?

KRISTEN ANDERSON: Unfortunately, we are just about out of time. So we just wanted to give you each a minute to close by sharing your thoughts about-- especially if you have any thoughts about best practices to protect consumer's privacy and security of their data, at least in these contexts.

CORA HAN: Should we go down the table.

CHRISTOPHER BURROW: Start with me.

Well, I think it's been a great discussion, and we've really focused on unexpected and, to consumers, unknown data flows that by these modern devices that we're all now acquiring can, if you will, leak out and maybe come back and have important effects. We've also heard that patients don't read privacy notices or consumers don't read privacy notices.

So I think we all have to work together to come up with some easier, better, more consolidated way to signal to people what are the risks that they're taking with their data and how they might mitigate those risks. And then each consumer chooses. On one end, Humetrix side Blue Button solution is providing, if you will, your own lock case for your own data that stays with you at all times, and you are completely in control of the data.

On the other hand, the Facebook example, if you are unwisely posting a lot of identifiable data there, that's really a bad choice. So I think it's going to be situational with regard to devices and specifically to apps.

I do believe there needs to be better and clearer information in the privacy policies presented in a very simple, graphical format that will give you a heads-up display right away when you use the app.

SALLY OKUN: Thank you very much. And this has been a delightful panel to be on. And I'm actually looking around the room thinking that people have questions. It would've been fun to get into some of those, too. So, so much to cover and so little time.

I think from my perspective, the most important, the last comment I would like to make is that we have to really try ways of reinforcing the value of sharing information to continuously learn about how to improve health and health care in this country. And trying to find ways of being able to do that by engaging with people and consumers on a regular basis about that value, and making that value equation come to life.

So shared data, along with share-- sort of allows you to have a more robust shared decision-making process, and ultimately, allows us to have shared accountability for the outcomes that we have. But also, the disposition of the data.

So I think it's a really important piece that as consumers each of us needs to start thinking more concretely about what is it that's constituting my role now in my health and health care, my family's role, my children's role, my grandchildren's role. And how do I help them appreciate and understand that value, while balancing and finding that area, that sweet spot, that says I'm exploring the risks as well and I'm beginning to understand them better.

But I do think we need to start holding a higher level of accountability around the use of apps and things that are sending data in places that may not necessarily be in our best interest. And until we can do that, I think, as consumers, we need to be much more aware of opting in, as Chris

said, or opting out, when it seems like our safety or the access to our information might be at risk.

KRISTEN ANDERSON: Sally. Joe.

JOE LORENZO HALL: Thank you, Cora and Kristen and FTC for holding this forum.

Similarly, I definitely think there-- the thing that, and this is almost a full employment act for myself, that it happens all the time. Is that when people want to do something cool, make a health app, make a thing that does something fun, they inevitably don't think about a lot of these things, unless they're developing a privacy app or something, a privacy and security app.

And so it would be really nice to have frameworks and have people develop sort of not just guidelines and stuff, but development environments, technical tools that would allow people who have a cool idea to not have to worry about some of the-- I mean to some extent you want them to worry a little bit about that, but it would be great to sort of obfuscate away some of these core security things. And security and privacy aren't that different, in that security enables you to protect your privacy.

And so I'd really like to see something like that that would-- and I don't know who I'm asking to do that. Maybe it's us, for example. Or in cooperation with some of the app industry folks. Because we want people to make cool stuff, but we also don't want to keep on having these common failures.

And I don't want to rely on enforcement entirely or the press entirely to sort of shame or whatever people into doing the right thing. But actually have some things that are sort of embedded into how these tools are created.

CORA HAN: Thanks. Joy.

JOY PRITTS: At first I was kind of regretting getting the end spot, worrying that I wouldn't have anything left to say. But I think it gives me a great opportunity to finish with what we have been using kind of as our public service announcement in some ways at many of the presentations that we go.

Because what's really-- one of the things that we find is really important is that everybody has a role to play in protecting this information. The government clearly has an important role here in establishing regulations that are both effective and that are workable for people.

The providers have, and the plans, of course, have their role in protecting the information when it's in their hands and when they're transmitting it. And then the vendors, the app developers, the device vendors, they're also responsible for building in privacy and security into their products.

And we can go on with all the other people or the entities that touch this, but it's really a cultural change that we're trying to make here. And it goes all the way down to the patient, because the patient is also responsible.

It's going to take a lot of effort for all of us to really bring about this change. I do think that we are kind of at a defining moment here. Although we've said that many times over the last several years. But there is a huge movement here with big data and how it's being shared, and how all this information is flowing.

And it's really mementos, and it's a very different than the way things were even 10 years ago. And I think that we're all responsible for sitting back and thinking how are we going to manage this in a way that's responsible.

CORA HAN: Thanks. So thank you all for coming. I think this is it. A special thank you to our presenters and panelists. We will be accepting comments on these issues until June 9, and instructions for submitting those comments are available on our event web page.

So thank you again all for coming.

Thank you.

[APPLAUSE]