U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH
INFORMATION TECHNOLOGY

ROUNDTABLE: PERSONAL HEALTH RECORDS
UNDERSTANDING THE EVOLVING LANDSCAPE

Federal Trade Commission Conference Center
Washington, D.C.
Friday, December 3, 2010
PARTICIPANTS:

Panel 1:

KATHY KENYON, Moderator  
Senior Policy Analyst,  
Office of National Coordinator for Health  
Information Technology

COLIN EVANS  
Chief Executive Officer, Dossia

TIM MCKAY, Ph.D., CISSP  
Director of Digital Identify Services CISSIP,  
Kaiser Permanente

LORI NICHOLS  
Director, HInet

GEORGE SCRIBAN  
Senior Program Manager, Microsoft HealthVault

GREGORY STEINBERG, M.D.  
President and Chief Executive Officer  
ActiveHealth Management (AETNA)

Panel 2:

WIL YU, Moderator  
Special Assistant of Innovations and Research  
Office of the National Coordinator for Health  
Information Technology

STEPHEN DOWNS, S.M.  
Assistant Vice President,  
Robert Wood Johnson Foundation (RWJF)

DARCY GRUTTADARO, J.D.  
Director, National Alliance on Mental Illness  
(NAMI) Child and Adolescent Action Center

JOHN MOORE  
Chilmark Research
PARTICIPANTS (CONT'D):

GAIL NUNLEE-BLAND, M.D., F.A.C.E., F.A.C.P.
Interim Chief of Endocrinology,
Director of Diabetes Treatment Center, Howard University

DOUGLAS TRAUNER
Chief Executive Officer, TheCarrot.com

Panel 3:

JOY PRITTS, Moderator
Chief Privacy Officer
U.S. Department of Health and Human Services

ROBERT GELLMAN, J.D.

JOSH LEMIEUX
Director of Personal Health Technology,
Markle Foundation

LEE TIEN, J.D.
Staff Attorney, Electronic Frontier Foundation

TRESA UNDEM
Vice President, Lake Research Partners

MATTHEW WYNIA, M.D., M.P.H.
Director, The Institute For Ethics,
American Medical Association

Panel 4:

LESLIE FRANCIS, PH.D., J.D., Moderator
Distinguished Professor of Law and Philosophy and
Alfred C. Emery Professor of Law,
University of Utah

LORETTA GARRISON, J.D.
Senior Attorney, Bureau of Consumer Protection,
Federal Trade Commission
PARTICIPANTS (CONT'D):

ADAM GREENE, J.D., M.P.H.
Senior Health IT and Privacy Specialist
HHS Office for Civil Rights

JOANNE McNABB, CIPP/G,
Chief, California Office of Privacy Protection

ROBERT HUDOCK, J.D.
Counsel, EpsteinBeckerGreen

FRANK PASQUALE, J.D.
Schering-Plough Professor in Health Care
Regulation and Enforcement, Seton Hall Law School

NICOLAS P. TERRY, B.A. (HONS.) LAW, LL.M.
Chester A. Myers Professor of Law,
Saint Louis University School of Law

* * * * *
MS. PRITTS: Can I get everybody to take their seats, please?

Welcome. It's good to see everybody here this morning. I am glad that we had such a good attendance for this event. We're very excited about our program for today. We have -- are we on the webcasting at this moment?

I'd also like to extend a welcome to everybody who is listening over the Internet. It greatly expands our audience, and we want to make sure that we include you in all of our discussion today.

We're here today to talk about personal health records, understanding the evolving landscape. Before we get started, I'm going to go over the necessary housekeeping details here to make sure everybody knows everything about what we need to do in case of emergencies, personal or otherwise.

So anyone who goes outside the building
without an FTC badge will be required to show your
ID again as well as go through all the security
again when you come back in. So if you leave,
you've got to go through the whole same process
when you come back in.

In the event of fire or evacuation --
pay attention here -- of the building, leave the
building in an orderly fashion. Now, this looks
like a good group. I think you can follow
directions, so I'm pretty confident that we can do
this.

Once outside the building you need to
orient yourself to New Jersey Avenue. Across from
the FTC is Georgetown Law Center. Look to the
right front sidewalk, that's our rallying point.
Everyone will rally by floors. We'll all just
rally together, okay? And then we'll just make
sure that -- we'll try to make sure that everybody
is out.

In the event it's safer to remain
inside, you will be told where to go inside the
building -- that's a loaded question.
Okay, if you spot suspicious activity, please alert security -- that's very suspicious activity, not somebody who's swiping your pen, okay?

The restrooms are located on this floor. You go out these doors here. You go out the main door that you walked in when you signed in and you will see where the guards are. You just job a little bit to the left and go down that hall and you're down there.

We have breakfast items that are still available until 9:00 a.m. Lunch items will be available for purchase in the hallway from 11:45 to 1:45, and we are very grateful for the vendor who came in to offer these items to us because it was not an easy process, and so we are very thankful for them who were willing to come in for a relatively small crowd and provide this service to us.

Importantly now, pretend like you're at the movie theater and please turn off your cell phone. Put it on vibrate or turn it off, and if
you need to use your phone, please go out in the hall to do so and stand away from the door so that it doesn't interrupt the proceedings. These proceedings are being videotaped so not only will you interrupt us now, you will interrupt us forever on the website. And if I know your name, I will say it.

WiFi is available in this conference room, and you can see the registration for further information.

Is there any other housekeeping detail that anybody feels a pressing need to know right now?

SPEAKER: Hash tag? Is there a Twitter hash tag for the Roundtable?

MS. PRITTS: I'm sorry?

SPEAKER: Is there a Twitter hash tag with the (inaudible)?

MS. PRITTS: Is there a Twitter? I don't know the answer to that?

SPEAKER: PHRR.

MS. PRITTS: PHRR?
SPEAKER: Yes.

MS. PRITTS: There you go. Somebody in the audience knew the answer. Good. I'm glad. I'll get you for that, Steve, okay.

All right. So now we're ready to get the show on the road, and it's going to be a fascinating day talking about personal health records. Here to welcome you this morning we are very fortunate to have -- we're very fortunate to have David Blumenthal, who has been leading the Office of the National Coordinator for Health Information Technology.

I've been at ONC now for since February, and I will tell you that ONC is not an easy organization to lead. It is like an Internet startup company, but in addition to having all those techie type of people, we have a whole concentration of doctors and lawyers, and, you know, I can't think of a more interesting mix to have in one organization, all of whom are sure they have the right solutions for the right problems and they're all different. So it's a
very good, exciting challenge. And David has his hands full on an hourly basis, and we're very fortunate to have him lead us from being a very small office to a much, much larger office in these really exciting times.

So I'm going to turn it over to David to make a few welcoming remarks. (Applause) DR. BLUMENTHAL: Thank you, Joy. Thanks to you and to all the ONC staff and colleagues that have been organizing this activity today. Thanks to all of you who have come. Joy is a terrific asset for the ONC in terms of the privacy and security, and other issues we have to deal with. Her post, as many of you may know, was created under the HITECH Act, the first time that the Department of Health and Human Services has had a chief privacy officer, and it's added enormously to our ability to focus on these terribly important issues and incorporate them into our planning the way they should be.

This program is part of a congressionally mandated activity for the Office
of the National Coordinator that we examine the
privacy and security concerns surrounding
non-HIPAA-covered entities.

You're having trouble hearing me?

SPEAKER: They just turned on the AC (inaudible).

DR. BLUMENTHAL: Is this better? This
would definitely be better. So I'm height
handicapped, and often the AV stuff just doesn't
work for me, so I will talk, I will bring the
microphone to me rather than move to the
microphone.

As I was saying, this activity today is
part of a HIPAA -- I'm sorry, a HITECH-required
study of the implications of the need for privacy
and security activities related to
non-HIPAA-covered entities and not -- and their
business associates. We're doing this in
collaboration with the Federal Trade Commission,
who -- which has very generously have given us
access to this facility for the day, and we will
be working with them over time.
As many of you know, they've also been active in the general area of privacy and security for commercial activities beyond the HIPAA rules and have published a report on that just this week.

The question of personal health records and other novel devices and mechanisms for moving patient and consumer health information around the health care system is a critical part of the larger challenge that we at the Office of the National Coordinator have to take on. And I want to just put it briefly in that larger context for you. The Office of the National Coordinator is charged under the HITECH Act with creating a nationwide, interoperable, private and secure electronic health information system. That's a lot of words. It's also a lot of work and a big challenge.

I try to remind my staff, when things look almost insuperable, that this is something that has never been done before. It's the equivalent of a Mars shot. So there are a few
countries the size of modest-sized states in the
United States that have made significant progress
along this route, and we are very happy to see
that progress, and it provides a great example of
potential routes to success.

But the idea of taking a country and a
health care system that extends from the Bering
Straits to Key West, and also out to Hawaii, and
making an information system that is
interoperable, private and secure, usable,
user-friendly, doing that in the modern world with
all the political and organizational and economic
challenges that our country faces, as well as the
appropriate and necessary demands for consumer
access and consumer protection and privacy and
security, that is truly a novel, unprecedented
effort at social change, the improvement of
society broadly. Our success will depend on at
least two things: First of all our ability to
relate, but then also our ability to stay constant
to certain important principles.

The innovation will include the
innovation and technology. The technologies that
we are here to talk about: the personal health
records, multiple devices, all the other things
that seem to spring up, suddenly becoming apparent
on the front pages of the paper and the tech
sections of the paper or in the technical
journals. Those are part of the key to our
success, and we want very much to not only be
receptive to that innovation but to encourage it.

Most of you, I hope, are familiar with
the meaningful use framework, that part of the
HITECH law that provides incentives for providers
of care to adopt certified electronic health
records and use them in a way that promotes
patient health and health system improvement.

That meaningful use framework has done already one
very, very important thing, and something that our
office can claim very little responsibility for,
and that is to set off an explosion of innovation
and the recruiting to the health sector of IT
talent that before had largely focused on other
areas of the economy.
So it's hard to see a day go by without hearing about some large IT company that is now making a commitment to the health space when before it was focused on completely different areas. It could be Intel, it could be Verizon, or it could be IBM, it could be Hewlett-Packard, it could be Google, or it could be Microsoft, but all these companies are flocking in, and even more interesting, there are just tons of new companies that didn't exist a couple of years ago that are bringing novel products to the market. And we cannot be successful unless that process of innovation continues. And where it will take us nobody can predict, but we will not be successful without it.

At the same time, while we allow and encourage that innovation, we have to be consistently constant in our commitment to certain basic principles. One principle is that the patient and the consumer come first; that everything we do is guided by its potential benefits and takes into account its potential
impact on the average individual, the patient who
every day contacts his or her provider of care,
whether it's in a nurse's office or a physician's
office, or a large hospital or critical access
facility, whether it's online getting health care
advice or shopping for -- online for a piece of
durable medical equipment, whatever it is. The
patient's interest, the consumer's interest has to
be a guiding light for us, and as part of that,
their faith in the privacy and security of what
they're doing, of their personal health
information also has to be a guiding principle in
our work to assure that that their faith maintains
strong and is justly placed.

Innovation will be one of the assets to
assuring that and containing that principle
because as technology improves, our ability, I
hope, both to advance the patient's interest in
information-sharing and the patient's interest in
privacy and security, our ability to advance both
those simultaneously we hope will improve.

Part of that, maintaining that
principle, is meetings like this one where these
issues are discussed in an open and transparent
way. We heard a lot about security in Joy's
introduction, but we are distinctly not making
this a private event. We want it to be open. We
want people to have access to this discussion, and
in the workings of the Office of the National
Coordinator over the last 18 months, we have had
well over 200 public meetings of our federal
advisory committees in which all the issues that
are before us have been discussed in the open, so
that anyone who's interested can tune in.

We hope this study will continue along
those veins and in an open and transparent way
continue the process of dealing with the most
critical, or one of the most critical issues that
we face, and that is to maintain trust in our
health information systems.

We have a terrific group of scholars,
experts, policymakers, and others here today to
help us with that work. We have consistently
benefited from the expertise of people in the
various fields in which we work. We could never have done what we have accomplished without them, so we thank you. We thank you for being here, we thank you for your continued commitment to the work we're doing, and we look forward to benefiting from your expertise.

Thanks again to Joy for organizing this, and I look forward to listening in as the discussion proceeds.

(Applause)

MS. PRITTS: Thank you, David. I'm going to do just a little bit of setting the stage here before we move into a main part of our program, and before I get that, I would like to point out -- Kathryn, could you raise your hand, please? As Kathryn Marchesini, if you have some issues today -- Jennifer, are you in the room, too? Lazenby?

Well, if you -- there she is -- there is Kathryn and Marchesini, and Jennifer Lazenby, and if you have questions or issues that you need help resolving today, they're here to help assist us.
They have been both very instrumental in putting this panel together and, among their other duties, they're just here to make sure that things run smoothly. So thank you very much.

So let's set the stage a little bit about PHRs and how health care and health information is evolving even as we stand here today. We're entering a period of which is almost like the perfect storm for the development of health information technology around consumers. We have all these general efforts going on for the adoption of health information technology and health information exchange trying to get providers to actually get the information into electronic form so that it can be easily shared with each other.

We also have health care reform and along with a lot of the efforts of health care reform that are centered on making sure that people have more access to care, that their care is better coordinated, that the patient is really the central focus of health care is the idea that
it is, and that the patient is at the core of that health care and has some responsibility for ensuring that health care and taking care of their own health in helping to ensure that their health care is coordinated, making sure that they are a part of the process here. It's not -- health care is not something that is being done to an individual; they are a partner in that, and that surely is part of health care reform.

In both of these efforts, the individual becomes key. It is not about - it is patient-centered care is what we're really aiming for. We need both the technology and the other incentives in order to make that happen.

We have a lot of efforts going on to make sure that the providers are brought into the system, so in our office in particular we have regional extension centers to help bring the health care providers along so that they can qualify for meaningful use payments, and really get them up to speed on electronic health records and adopting this new technology. They are also
working with some of the critical care hospitals.

We also have efforts at the state level to help bring, make this a coordinated effort on a more regional basis so that the information can actually be shared regionally at the state level. So we have at that level, level of the providers and at the levels of the administrators, and we're making a lot of efforts in those areas.

So what are we doing to help the individual because right now the way most individuals take care of their health information, if they do it all, is with a paper file, or boxes, or a bag full of prescription medications that they take in to the doctor and say, "This is what I am on." And I think we've all concluded that that just is not acceptable anymore. That is so 19th century and here we are in the 21st century, and we really have to make a little progress in this area.

So some of the ways that we are going to -- that we're making efforts to help the patient in this whole effort are set out in meaningful
use. For those of you who are -- I can't believe anybody in this crowd would not be familiar with the meaningful use terminology, but meaningful use relates to the fact that if a health care provider meaningfully uses an electronic health record, they will receive incentive payments? And as part of that effort, they are going to be expected to give patients access to their own health records.

HITECH also focused on patients in particular, and there are provisions in HITECH that provide for the electronic access of information upon a patient's request. There are also portions of HITECH that address PHRs and similar technology, in specific. Congress recognized that there is a burgeoning effort in this area and wanted to ensure that at least that the information -- at the very least -- that if the information was breached, if there is a security breach or it was obtained inappropriately, that the individual would be made aware of it.

But Congress was also concerned about
whether there are other, potentially other requirements that might be necessary in order to continue to protect this information as we move forward, and as part of that they required that this study be done to inform them of what should, if anything, should be done with respect to protecting the privacy and security and the safeguarding of health information as it moves beyond medical records into these other forms of transferring and using health information.

We have in the United States a very sector-driven approach to regulating health care, and what that means is that our laws are written so that they apply to doctors, to hospitals. HIPAA itself is somewhat sector-driven and applies to health care providers and health plans and health care clearing houses, and now with the amendments at HITECH also to business associates. But we all recognize that that still leaves some gaps in protecting of the health information.

So we have a lot of information, we are encouraging it to be shared, and there are a lot
of things going on here, as you will soon learn
from the panels coming up, but a lot of it raises
what -- a new but also what I would call an
age-old question -- which was posed by Thomas
Jefferson, who had said that our laws and
institutions must keep pace with the progress of a
human mind. Well that is quite a challenge today
when we look at the differences in even what a
computer -- a flash drive.

When I started using a computer, I'm
ashamed to admit almost that we used punch cards,
and in my lifetime we've gone from the computer
capability of something that's in a room can now
be held on a flash drive that's this big. And
with that kind of change, it's very difficult for
the policy to stay up with the technology, but
that's exactly the challenge that we face today.
That's exactly the issue that we're looking at
today is how are we going to be able to strike
that right balance between maintaining the
innovation but making sure that the information is
being used for the purpose that the individual
believes that it's being used for and has agreed that it should be used for.

In order to do that, we have four panels with us today. We have some amazing talent in this room, and we are very grateful that everybody was able to join us.

Our first panel is -- we will introduce all of the individuals speakers by the panel -- so that you will have a better understanding of how they fit into the scheme of things. In our first panel, we'll discuss PHR origins, developments, privacy and security practice. They will be followed by a panel that addresses the new forms, the new audiences, and the new challenges of PHRs.

After our little lunch break, we'll have privacy and security of identifiable health information in PHRs and related technology, the expectations and concerns, and then our last panel will address the perspectives on privacy and security requirements for these PHRs and related technologies, and they'll explore a little bit about what the current state of regulation is and
whether any additional, any additional means of
protecting the information, whether it be
self-regulation, industry standards, legal
regulation, those types of things are required and
necessary, or may they actually impede
development?

We'll then have a brief period for
public comments.

So I'm glad to have you all here. I
think it's going to be a long and very interesting
day today, and we're going to start with our first
panel, if they can come up to the stage, please.

Our first panel today addresses the
origins, developments and privacy and security
practices in PHRs. We are sorry to say that Jodi
Daniel, who was originally scheduled to present on
this, to moderate this panel, is not able to be
with us today. She has been ill week. In her
stead we have Kathy Kenyon, who is very familiar
with this area. She's been working very hard with
us over the summer in putting this panel and some
of the other panels together.
Kathy is a senior policy analyst at ONC's Office of Policy and Planning. She works with Jodi in that role. She's been here with us for about 15 months now. She's an old hander by ONC standards. She comes with 23 years of experience as a health lawyer working mainly with large provider organizations that have been early adopters of health information technology. And at ONC she works on consumer engagement and patient safety issues among other things, and we are very grateful for her for being here today and stepping in when she was needed and for helping us just in general. And she will moderate this session and introduce her panelists.

Thank you, Kathy. (Applause)

MS. KENYON: Thank you very much. First I want to extend Jodi's regrets. I heard from her by e-mail this morning, and she has no voice, but she would have loved to have been here.

The panelists we have here today will help us understand the origins and business models of different approaches to personal health records
with special attention to the privacy and security practices. Each panelist represents a distinctive chapter in what is really a very brief story of PHRs. Kaiser Permanente, represented by Tim McKay, who's Director of Digital Identity Services, Kaiser, of course, has been a leader among large integrated health systems in use of electronic health records and in development of ways to get information to patients, including through personal health records.

Tim has been a part of Kaiser Permanente's Internet Services Group since 2000. He began his career as a pediatric clinical psychologist and applied researcher in population health management. Today he's responsible for Kaiser's flagship website, which is KP.org. That website hosts more then 3.2 million active personal health record accounts for Kaiser Permanente's 8.6 million members.

The next is Shared Care Plan, represented by Lori Nichols. She's Director of Whatcom Health Information Network and represents
a community-based approach to PHRs driven both by providers in the community and consumers. Whatcom County in Washington is north of Seattle and south of the border with Canada, as I understand it.

MS. NICHOLS: Just barely.

MS. KENYON: I understand, okay. Ms. Nichols has served as program director on six different major grants to build an E-health infrastructure in Whatcom County in areas such as health information exchange, E-prescribing and a person health record bank pilot.

Then we have Active Management PHR. It's represented by its President and CEO, Dr. George Steinberg.

DR. STEINBERG: Greg. Gregory Steinberg.

MS. KENYON: Greg. No, it's not, not George, Gregory.

DR. STEINBERG: It's all right.

MS. KENYON: And ActiveHealth Management has its roots in Aetna Healthcare, but it's moved front and beyond that, and we'll hear more about
that later. But its roots in Aetna means it's based in a covered entity. Obviously, health plans have been major drivers of PHR development, so he represents that perspective.

Dr. Steinberg is a cardiologist who is also an associate clinical professor of medicine of Columbia University and a senior attending emeritus physician at St. Luke's Roosevelt Hospital in New York City.

The next panelist is Dossia represented by its CEO, Colin Evans. It's a PHR company that was established by large employers as they try to address the health care needs of their employees. Colin Evans comes to us initially from the United Kingdom. He became Dossia's CEO in 2009 after 29 years with Intel where, among other things, he served as the Director of Digital Health Policy and Standards. He's been deeply involved in industry standards initiatives and has led research on virtualization, trust and content protection technologies, and on the development of platforms for home health monitoring.
And finally, we have Microsoft HealthVault represented by George Scriban, who's a senior program manager. Of course, Microsoft HealthVault is one of the best known vault model PHRs by a major technology company. Mr. Scriban has been involved in the business side of technology for 15 years and is responsible for product strategy, marketing, and planning for the core Microsoft HealthVault platform with regard to privacy, security, and compatibility with industry standards. This is a relatively new and dynamic industry, and the panelists today will help us see it from their perspective.

And with that I think we're going to move right into some of the questions.

Now, the format for this in each of the panels is going to be kind of I'm going to ask questions, but these won't be new to the panelists. The panelists know what the questions are, and so they've kind of planned their answers. I'm hoping that we get some interaction because, as it turns out, they know a whole lot more about
PHRs than I do. And so, you know, it's okay for,

once I have a question, if you think that you need
to make a point about how you're different or like
the other people who are here, please feel free.

So I'd like to start by asking each of
the panelists to describe basically their story.

Now, of course, we've given them two minutes to do
this, so, you know, they may have some difficulty
in that time frame. But basically, you know, what
are the origins of your PHR basic functionality?

How and why do individuals use it? How is it
similar to or different from other personal health
records?

So I think what I'd like to do is start
with Tim, with Kaiser.

DR. McKay: So most of you know that
Kaiser Permanente is a nonprofit organization and
that we serve eight distinct regional areas. And
a lot of our history of the PHR is based on our
organization, so if we look at the origins in the
beginnings, it really started in the mid-1990s
when we had the emergence of the beginnings of
electronic medical records systems, stubs in a number of our different regions. Of course, we weren't on the same system in any of the regions. We had the emergence of public websites so that they were mostly informational directory services, some health information, but again they were regionally based.

And then we had a national initiative that was looking at what kinds of secure services could we offer to our members, and those services began, launched in the mid-to-late '90s.

By 2002, though, as a company we made a decision to standardize on one medical record -- electronic medical records system -- and that was an amazing decision, and we are just now at the point where we've realized the fruits of that decision where we have electronic medical records rolled out to all of our service areas, and it's completely integrated into our medical offices and operations.

So along with that, we had convergence in our public websites from one, from a
regionally-based system to a national system, and we integrated our secure services with our public services so that if you go to KP.org now, you can cruise, use many of the services until you get to something that's secured, then you're challenged. And we decided to try to make it as naturalistic for our members as possible so that they would access the services that we need -- we would authenticate identity as we needed to.

I would say at this point we're at the beginning of a phase of maturity, so our services that we offer on the site are around health improvement and health information, like many providers and PHRs will have health and drug encyclopedias, total health assessment that will then integrate back into the electronic record that can be viewable by our providers; condition management programs, the use of health alerts for preventive services, directory services, claims and plan management services.

But then we get into the really interesting stuff to be able to view parts of your
medical record for seeing your allergies list,
your medications list, your problem list,
immunizations, lab test results all of which when
you see information, we hyperlink into information
that's in our health and drug encyclopedias to
give further explanation of tests and procedures.

We also have the ability to make proxy
assignments so that if you, as an account holder,
want someone else to be able to view your record,
you have the ability to do that. There's also,
then, a suite of transactional services, of arts
refill which integrates into a robotics
fulfillment system, a real-time appointing so you
schedule the appointment that you're actually
going to see your primary care provider for, and
secure messaging services where our patients have
the ability to message physicians, nurses,
pharmacists, psychologists, and other care
providers.

We're often asked, now, do you have a
personal health record, or is this a patient
portal? Our best answer to that is yes because we
truly have a shared, integrated record so that the
information that our patient sees is the
information that our doctors and providers see and
use. We are seeing our systems as continuing to
evolve, and our emphasis has been on operability
before interoperability, and we'll be able to talk
about some of the interoperability and patient
controls, I think, later on in the discussion.

But I think at this point that's -- my
two minutes are up.

MS. KENYON: Thank you very much. Lori,
let's talk about Shared Care Plan.

MS. NICHOLS: Okay, sure. So we're not
quite as -- well, we've had an EMR in our
community for since 1996, but we're not a single
organization, we're a community of various
independent practices. We do have a single
hospital, so we actually have 80 percent adoption
of EMRs in our community, but that's silos, that
doesn't give tools to patients. So in about 2001,
we were participants in a Robert Wood Johnson
Foundation-funded grant, Pursuing Perfection
grant, and in the interest of being patient-centered, one of the six aims of the Chasm Report, we had patients at the table, and we asked them what we wanted. And we were ready to expose the hospital's record to them, and they said thank you very much, we want our own.

And so we started out in 2002 building -- you know, starting with a word document, what do you want to track? And migrated through an HTML version, and now we have a very robust application that can accommodate web services interactions that's connected to HealthVault. We're about to roll out SmartPhone versions so patients can track, and they can see information from within the hospital system. We're working to integrate some additional EMR data feeds. And with the connection to HealthVault, any system that connects to HealthVault then can have that information show up in the Shared Care Plan.

Patients have a very granular level of control over who has access to what in their plan, so they could grant a general level of access to a
family member. That's the reason it's called "shared" is that patients really did want to share it with their small social network that helps them manage their care when they are not in the practice, when they're not in the hospital because really, we expect patients to manage their health on their own, and they have very few tools. It's so exciting to see this room and participate in this event. We're focusing on making tools available to individuals and their families and those they care for.

So we do have integration to our state immunization registry. People can print out the certificate of immunization form for schools, integration to HealthVault. As I mentioned, integration of lab results into the record, and patients can, with all of the talk about technology, I really want to emphasize we can't get rid of the value or dismiss the value of paper. People can print out a paper summary that folds up to a credit card size piece of paper, and if you're down on the street and you look through
your pocket, a flash drive's not going to do you a
lot of good, but if they have something that they
can read, that would indicate who they should
call, what meds is this person on, and what
diagnoses.

People have that ability to control
their information at a granular level, they can
say you have general level of access but you can't
see a particular medication. What else? We're
also building the technology to support workflow
transitions because people don't exist. Kaiser
has kind of a golden world where everybody -- all
the care really does happen kind of within one
organization.

In our community, even our large
northwest HMO is pretty much like any other payer,
and access to those kinds of systems doesn't
exist. So we're creating tools for patients to
help them bridge the gaps between practices with
calendared reminders and rules-based alerts, you
know, enter your blood pressure, what if it's
missed? What if it's out of range? Who do we
notify and how, so we can support SMS messaging or
messaging to e-mail or ring a phone.

MS. KENYON: Lori, what kind of adoption
do you have? I mean with all of this wonderful
functionality, are people using it in --

MS. NICHOLS: People are using it. Our
community is just under 200,000. It gets bigger
every time I say it, and we have about 2,200,
2,300 active Shared Care Plans.

There's a reason for that. We have not
intentionally really tried to push it because we
knew it wasn't ready. We started out when we
built the initial version. It was built as simply
as a chronic care tool for people to track their
chronic conditions, and we're building more and
more functionality to support robust active
healthy people to help them stay that way. And so
with the connection to HealthVault, that really
helps where people can download their exercise
watches and to help support care in the home --
glucometers, blood pressure cuffs, that sort of
thing. Downloading data from those is really
where we're going to really start to feel the
benefit of having technology for patients that
interacts. It's not about providers having EMRs
and patients having PHRs; it's how they interact
with one another and how the data flows, and try
to get some efficiencies through collecting
information once and using it over and over.

MS. KENYON: Okay. Thank you so much.

Next we're going to go to Greg, and there is logic
here because for those of you who know HIPAA,
Kaiser Permanente is a covered entity and so my --
you're covered by HIPAA.

DR. MCKAY: Yes.

MS. KENYON: Right. We go to Lori, who
starts with a provider based in the community, so
also a covered entity, but there is some
straddling between HIPAA and non-HIPAA as I
understand it, and we'll talk about that more.

Next we're going to go to a health
plan-based PHR model, and that, of course, is also
a covered entity, but we're going to see how it
moves into the non-covered entity world as well,
so, with that, Frank.

DR. STEINBERG: Okay, thank you.

Probably worth going through a very big history of ActiveHealth Management and trying to make the distinction between that and Aetna, so ActiveHealth Management was formally incorporated in 1998 with private venture capital funding.

We are in the business of providing clinical decision support services to various groups. We initially started as providing those services only to physicians. We had a number of health plan clients and large employer clients. One of those health plans was Aetna. They started in about 2002.

In 2005, they did the Remington Razor thing where they liked it and bought the company, and we -- but we function as an independent stand-alone business, so we provide our services to Aetna and Aetna members, including but not limited to the PHR. But we also provide those same services to a whole host of non-Aetna health plans and other -- and large employers.
The PHR was really born for us in about 2007. It came out of an articulated need by our various customers that we needed to have a consumer-facing, user-friendly and intelligent tool that would help patients, individuals make better health care decisions. We believed that -- the way we look at it is that the PHR is part of an integrated suite of decision-support enabled products that are designed to improve the overall quality of care by helping doctors and patients make better and more informed decisions about their care. We view it as a really a member-engagement platform that promotes health accountability.

In the PHR, one of the main features is that it provides patients with an intelligent, prioritized, and crisp sort of to-do list that's based on an intelligent analysis of all the data that we have on them, which includes data that we get from the health plans, data that we get from the PBMs, data that we get from labs, and obviously the data that individuals enter
themselves.

There is pretty robust clinical decisions support that is truly in real time, so what that means is that when you're in the tool and you complete our health risk assessment, and you press Submit, all of that information that you've just entered goes back into our systems, is appended to the data that we already have on you from the various sources that I mentioned, it runs up against our sophisticated clinical rules engine, and to the extent that a clinical alert needs to be generated, it goes back into your PHR. Everything that I just said happens within one second.

MS. KENYON: And the clinical decision support you're talking about is to the individual.

DR. STEINBERG: To the individual.

MS. KENYON: The individual, we usually think about CDS in terms of supporting physicians.

DR. STEINBERG: It is both. So the individual gets the message back electronically within one second; the physicians get their
messages through a variety of means, electronic
and sort of more standard, more standard ways.
The PHR and the content is fully
integrated with our other so-called care
management products, so our decision, our disease
management product, our health and wellness
coaching, all of that, and those systems talk to
each other so that data entered in one system is
automatically populated into the other system.
And then the last thing that I'll say is as we are
entering the new era of health information
exchange, we are entering into arrangements with
groups where, in addition to those other kinds of
data, we are receiving data directly through those
health information exchanges into our systems and
providing information back out through the health
information exchanges to the appropriate folks.
I'll stop there.

MS. KENYON: Thank you very much. I
think Dossia, Colin?

MR. EVANS: Sure. Okay, good morning.

Thank you. Thanks for inviting us to 201st
meeting of the various people discussing national
health infrastructure.

And so Dossia was founded by a number of
large employers that are concerned by, you know, a
health care system that has costs spiraling out of
control and a quality that's indifferent and no
hope of changing. So I think the way Dossia got
started was these employers wanting to found a
system that would help try and reverse that trend
a little bit. I mean, the health care
inefficiency is sort of a tax on every business
and every employee in America, and we want to try
and change some of that.

The system was founded on really two key
principles which I think we're going to hear
discussed a lot today. One is that an individual
that's empowered and informed and engaged in their
health is likely to make smarter health care
decisions and likely to be a more demanding
consumer of health care, and consumers have
changed every other industry in terms of
efficiency and cost, and we hope we will do some
of the same things in health care.

The second key principle that we're founded on is that employers, as payers of health care, have got some influence in making sure that the data can be made available to employees because, you know, employees pay the bills and they should have some influence on the people in the system. HIPAA and ARRA, as has been pointed out, give everybody a right to a copy of their information. We're just acting as a repository for that information in a secure and private way, and we're acting as an agent on behalf of individuals helping them collect their information from the different sources whether it be institutional data or biometrics, or devices, or self-entered information.

We aggregate information from different data sources, and we serve as a platform to launch, theoretically, an infinite number of different applications and services that can sit on top of that platform. And why would somebody use that? I think you have heard some of those
examples from the panelists already. I think
generally, you know, safety care coordination,
convenience, the ability to care for others are
all some of the key drivers that we hear from
people in wanting to get access to their
information.

MS. KENYON: How many people use
Dossia's PHR?

MR. EVANS: That number's all over the
place. We've got in some companies that have
rolled Dossia out to their employees, they have
done so without incentives or without any
particular drive. And they've got, you know, 10,
15 percent of their employees signing up. And in
other cases there are companies that have got --
rolled out a Dossia link to their other incentives
that are tied to other reduced health care costs
or the benefits they get, and the adoption rates
have been much, much higher from those companies.

So it ranges everything from 10 percent
to 80 percent, depending on whether incentive's
involved, and it's, you know, it's a big circuit
and we can get into that later, maybe.

So it's currently offered to employees of our founders, of our customers. You can't go to a website and sign up for a Dossia account. One of the benefits of doing that is that we've got very high capability to authenticate people as part of a health plan where you can't put Barack Obama or Donald Duck into our system and set up a health record. You have to be who you say you are.

It also allows us to maintain a very close control over family recognition so that someone that is covered by a health plan can also identify their, you know, other dependents, spouse, their kids, and so forth. In fact, in our last open enrollment at one of our customers, we had more kids enrolled than adults because people were adding their children.

I think somebody pointed out to me once that most people's family priorities are the kids, the wife, the dog, me, you know, is usually what people's priorities are. So the gathering family
information is pretty important to people.

I thought it was interesting that -- and
I'm sure we'll talk about this more later -- that
the FTC issued a report this week on consumer
privacy. I thought that was highly appropriate to
today's dialogue, and, you know, I'd
wholeheartedly support all the recommendations in
it. And it's easy for me to say because we built
out system basically based on those
recommendations. So, you know, I'm pretty pleased
that they finally got written down. I think, you
know, the kind of patient ownership of data,
transparency, and all those kind of things that
are built into those rules are, you know, clear up
front. Conspicuous rules are pretty key to us.

And I think, you know, just in closing,
I'd say I hope my -- my hope for the day is that,
you know, I think HHS and FTC in pulling this
together is a pretty interesting combination of
groups, and there's two responsibilities that I'd
like to hear discussed today: One is clearly we
need to set standards and rules for the
expectations of people managing their own data in
a real private way; but I also think that, you
know, FTC particularly has a responsibility to
make sure that privacy is not weighed spuriously
by many plays in health care as a barrier to
getting people their own information, or as a way
to stifle competition.

I think, you know, data should be,
should belong to the individual. The law's pretty
clear on that. You know, we implement a system
and make that happen, and I hope we can, you know,
move strongly in that direction through the
scrutiny of today.

MS. KENYON: Thank you very much. One
of the things that the last reflection there I
think demonstrates is that we clearly moved from,
you know, three organizations that probably, you
know, may look a lot to the OCR, to the Office of
Civil Rights, and HIPAA regulation -- except, of
course, Greg is probably in both camps more -- to
Dossia, which is not based in covered entities.

MR. EVANS: Well, but I think that's
kind of a myth. I think, you know, we've -- we're
receiving data from them. And employers,
self-insured employers' plans are covered
entities.

MS. KENYON: Oh, okay. good point.
MR. EVANS: So if we're working on their
behalf for the most part, we're a business
associate, or if, whether we have an agreement or
not, the law seems pretty clear that we're going
to be treated like a business associate. So, you
know, HHS and the FTC is an interesting sort of,
you know, dual-headed monster here because, you
know, Dossia could have a business associate
agreement written with every doctor in America,
and the FTC could still throw me in jail, all
right, because I'm making promises --

MS. KENYON: Do you have criminal
authority? Do we have --

MR. EVANS: I believe so.

MS. KENYON: Yes, we do.

MR. EVANS: I mean I'm making -- you
know, my system's making promises to consumers
that we'll preserve and protect and maintain their
information whether, regardless of what HIPAA
says.

MS. KENYON: Oh, okay.

MR. EVANS: So I think, you know, we're
covered by both.

MS. KENYON: We're laying the foundation
for Panel 4 here, so -- okay, and then finally I'd
like to turn to George Scriban from Microsoft
HealthVault.

MR. SCRIBAN: Right. So Microsoft's
interest in the personal -- in the health care
space has been driven primarily by the, I guess,
the principle that pivoting the health care system
and pivoting care around the patient requires some
- a different set of tools than ones physicians
and providers have been equipped with to date.
And that's part of what my group at Microsoft, the
Health Solutions Group does. It's solutions to
help transition, you know, providers to
patient-centric care.

On the patient side, that's where
something like HealthVault comes in. What we also
realized is that, you know, individual patients
ourselves, you know, individual consumers, we're
not really enabled to manage the fragmentation and
the diversity, and the sort of the sheer volume of
information about us that is produced by our
encounters with the health care system, much less
the stuff that we generate ourselves, because
health care happens 365 days a year. It just so
happens that 300-some, plus some-odd days, it
happens without doctors and nurses present with
you; it happens with your family. And it happens
about, you know, with your family and caregivers
in the community, and, you know, and it's -- and
it happens kind of among your family as well.

So there's this need to not only
coordinate and aggregate all of the information
about yourself as an individual patient but to do
so for your entire family, because, generally
speaking, there's one or two people within every
family that manages health care decisions and the
health care processes for every family.
So this is -- that was the genesis of HealthVault. We spend time with consumers. We spend time with the family health manager, generally speaking, you know, moms in families, and looked at the way they managed health information. And, as everybody knows, it's in boxes. To the extent that they can collect the stuff, it's on paper in boxes spread throughout the house; it's never where they need it to be, it's never in the format they need it to be in. And it doesn't really help them even if they aggregate it. It doesn't really help them manage in the day to day.

What we created with HealthVault was a completely consumer-controlled, cloud-based service that allows consumers to collect and store their health information. And we created interfaces that allow entities within the health care world -- providers, plans, PBMs, labs, device manufacturers -- all these different players that have information about you, all these fragments of information about you to contribute data under
your control and at your request to your
HealthVault record.

These interfaces also enable third-party
services to help you day to day. So third parties
ranging from the American Heart Association to the
American Cancer Society, to the Mayo Clinic, the
Planned Parenthood, have all developed to little
start-ups, have all developed applications that
help people with HealthVault records manage their
health care.

So the AHA, for example, developed an
application called Heart 360. It's a pretty
interesting, reasonably straightforward way of
managing your cardiovascular health using the data
that's in your HealthVault record. And that data
can come from any place, right. It's all
aggregated into this single platform. It can come
from your providers, it could come from your blood
pressure cuff device that's HealthVault compatible
that you could buy it at a drugstore. And in so
doing, what we have done is we've taken the burden
of collecting and controlling this information,
protecting it, ensuring that consumer wishes with regards to privacy and security are respected, and we have taken that burden upon the platform, onto HealthVault and freed up the third parties like the American Heart Association to worry about delivering the smart stuff, right?

So we never -- we -- so, interestingly enough, I'm sitting here on a panel discussing personal health records. We don't really consider ourselves a personal health record. It may be a fine distinction, but what we consider ourselves, consider ourselves to be a personal health information platform where the brands and the services that individuals trust to deliver health information and health advice will come from other sources. Basically, this is just my fancy way of saying I don't think anybody ever -- at Microsoft ever predicted or expected people to think that Microsoft's going to help you manage your diabetes, probably because we would give it a terrible name like Microsoft blood sugar, you know, 2010 released to consumer edition.
I kid. I kid because I love my marketing department. But because people trust other entities, whether it's their personal physician, their community hospital, or Mayo Clinic, or Johns Hopkins or whomever, implicitly more directly, and we didn't want to get in the way of that relationship. What we did want to do, though, was make sure that there was a place where we could exercise as consumers, exercise our right to our -- to obtain our health information and make it useful in some way.

MS. KENYON: You know, my next question as I've, you know, have gone, as we've heard this, is profoundly naive because it was about how we've moved away from the original vault style model of a PHR into, you know, something that has a lot more functionality for patients. And I think that what we've just had described by George is that movement. You are not just a platform for -- a repository for information anymore.

Now, my sense -- let me ask the others to tell me the extent to which that, what George
just described with HealthVault in terms of the connections to an AHA-developed application, is happening. My sense is that other people are bringing in the apps in the same way. Am I correct?

MR. EVANS: Yeah. I mean --

MS. KENYON: (inaudible) Dossia?

MR. EVANS: -- I think we're probably closest to HealthVault architecturally. I think absolutely we're doing that. We're -- it's an open-ended system that's intended deliberately, as George said, to provide the data that someone's got in a way that they can control who sees it, where it goes to, who they're accessing and then enable that to be used by any number of people to make sense out of it.

MS. KENYON: And, Greg, is that pretty much how you're --

DR. STEINBERG: Yeah. We actually have the capability-- we have embedded the capability in our PHR for members at their discretion to actually upload their data directly into
HealthVault.

Interestingly, you know, we have between the 8 million members that are Aetna and the 2 million or so members that are not Aetna on our system, I don't have the exact numbers, but it's not a lot of those members that have, for whatever reason, elected to do that.

MS. KENYON: Okay. Tim, for Kaiser, because you're more of a control system --

DR. McKAY: Sure.

MS. KENYON: How did -- do people have the ability, if they leave Kaiser, to take a PHR with them? How do you transition that?

DR. McKAY: So there are a couple of things. So folks right now have the ability to download their information into a summary that can be then printed off, saved as a PDF or put on a USB memory stick. In fact, many of our medical offices provide those password-protected sticks for people to carry and put on their key chains.

What we're starting, a large initiative, and most likely we're going to start it at the end
of next year, we're expanding our whole identity structure so that it's going to be inclusive of not only our members but nonmembers as well. And we're looking at identity more as a lifecycle -- that people will come in and out of membership, have needs at different times, and we want them to be able to get access to their historic information even when they've left our plan.

As we get more mature in interoperability, we expect that it will just be common course for people to download their information to some trusted source under the consumer's control and to be able to take that information with them and then reapply it to a new health plan.

MS. KENYON: Mm-hmm. Are you building access to apps from outside --

DR. McKAY: Yeah.

MS. KENYON: -- companies into Kaiser?

DR. McKAY: In fact we already have. We do contract with a few different companies that are our business associates that provide certain
services that provide certain services. And the
-- in fact, right now we're completing about a
three-year redesign of our website to make it more
service-compatible so that it's easier to plug in
applications from other providers to do
distributed developments. And we, because as
Internet Services Group, we -- our mission has
been to provide a core suite of services and
realized that as new needs come up and they emerge
in new technologies and new services, we want to
be able to adapt those into our site as quickly as
possible.

MS. KENYON: Okay. I'm going to move
now to asking a little bit about the business
model. Let me get one thing clear to begin with:
Do patients, do individuals who have a PHR ever
pay for that? Is the payment for it ever coming
out of an individual's pocket? No? Okay. That
-- that I've -- so clearly when we move into
talking about a business model, we're not talking
about a business model that the individual owner
of the PHR is paying for. That means that you're
getting your resources from someplace else.

So I'm going to ask you to talk about what is the source of revenue to sustain your PHR. Have you been growing? Has the growth met your expectations? You know, what is the business model that might sustain your PHR?

And I think that I'll just start at this end this time with you, Colin.

MR. EVANS: Okay. All right, keep us on our toes.

MS. KENYON: Mm-hmm, yes.

MR. EVANS: Well, Dossia is, you know, was founded by employers, so we get paid by those employers to provide a benefit to their employees so that we get paid subscriptions on their behalf and to -- so the employee themself sees the solution at no cost to them, as provided by their employer. And we are also in conversations with other potential users of the platform providers and plans also that would have a similar model or similar rationale for providing that kind of untethered system.
Our business model is based on the
system being untethered from other parts of the
health care system. We're an independent
repository of information. Ultimately, we're
under a not-for-profit umbrella, and the Dossia
Consortium is an organization that's, when we set
it up, it was very important for us to make sure
that employees would realize that the system would
not have its motives compromised by, you know,
inappropriate business goals. You know, trust in
the system isn't just a question, you know, of
privacy and security technology; it's do you
understand what someone's doing with this
information and why they're doing it?

So we're founded as an, you know,
independent organization from the employers
particularly.

In terms of growth, yes, we're rolling
out to more and more employers. We just rolled at
AT&T and BP and we've got, you know, most of our
founders are rolling the system out. The level of
adoption is -- varies depending on the particular
program that an employer is using. Some are interested in getting a lot of people to do a little bit on the system; other employers focus more the particular employees that are sort of frequent flyers in the health care system because that's where the money is, and that's where the benefit could be. If you actually help somebody manage their care, you make someone's life a lot better, and you actually save a lot more money for them and for the company.

So different companies have got their roll-out models. It's really not easy to talk about a percentage of adoption because they have different business goals.

MS. KENYON: And so Dossia is one tool that employers might use to help their employees control their --

MR. EVANS: Typically, we're kind of a launch platform for wellness programs for employers. They've got -- they certainly would have just general, you know, health risk assessment employee engagement, but they also
might use it as a launch vehicle for particularly,
you know, a diabetic program for disease
management or smoking cessation.

MS. KENYON: So you're --

MR. EVANS: Or some companies link it to
their on-site clinics; some companies link it to
their on-site fitness centers. We've got feeds in
from exercise bikes, all right, in on-site
exercise facilities.

MS. KENYON: To a very different
business model. Tim, explain.

DR. McKAY: Sure. Our model, we get our
funding from our member dues. And, honestly, we
approached the whole PHR space in the evolution of
our Web portal as more of a social mission,
frankly; that we were focused on meeting the
health and improving the health of our members in
our community, and that this is one step in being
able to do that.

What we do find is that there is offset
to some degree for the services that we provide.

So if you think that when a person gets a lab test
result, and the process of getting that result
written down, put in an envelope and mailed, it's
easily, when you look at the work flow cost, it's
a buck, a buck a pop when they go out. And if you
look at 25 million lab tests, the results being
resulted online last year, that's substantial
savings.

Now, the caution is that the more
distributed your program is, the more distributed
those savings are going to be. So, honestly, you
see more savings in terms of work flow
productivity than you can attribute to any
particular cost center. So we see those in
pharmacy refill, in direct booking as well.

Our growth has been surprising to us,
honestly. We know that these services were good,
that we had really put a lot of time and
investment in them, but we have grown, for
example, from 2006 with 20 percent of our eligible
members having a current account, to this year
having close to 60 percent of our eligible
members.
But registration and account growth is really only one metric, so if we look at our account growth from last year to this year, about a 20 percent increase. But we've seen a 40 percent increase in actual use. So the more that people have exposure to the tools, the more that they're promoted within the doctor's office, and it's very much a part of the natural work flow. So you go into the doctor's office, the physician has their terminal that they are writing their progress note, they're looking up information, they're maybe sharing information with you on the screen, and at the end say, you know, I really want to hear about how this is going for you. Can you send me an e-mail in a couple of days? And there's kind of an expectation that our members have these tools at their disposal and that the system as a whole promotes its use in a very naturalistic non-coercive way.

MS. KENYON: And so you've directly reduced some of the cost of doing business.
DR. McKAY: Yes.

MS. KENYON: And you've also, you know, promoted better quality care which can reduce cost in a Kaiser model.

DR. McKAY: I think one of the interesting things about a shared record when you know what you're seeing that the provider is also seeing, that if you're seeing something as a patient that isn't correct, you have the ability to facilitate getting that corrected quickly. And we find that the patient's safety alone of exposing that information is well worth the cost of the system.

MS. KENYON: Okay. Fabulous. Lori?

MS. NICHOLS: The development so far has been largely grant-funded. We've reached the point now where we're going to roll the cost of our ongoing support into our regular access fees for our intranet. And I kind of nodded in a delayed fashion to the no-cost-to-consumers because it is free to consumers and our Web version will be. But as we roll out the
SmartPhone versions, there would be a small charge for that. And we're also looking.

MS. KENYON: - Now the small charge would be paid by...

MS. NICHOLS: By the consumer to download the app.

MS. KENYON: Okay.

MS. NICHOLS: Because they do it all the time.

MS. KENYON: Yeah.

MS. NICHOLS: There goes another 99 cents. So, and then we're also looking, as we build out our work flow functionality, especially supporting transitions from acute care settings to out, that hospitals will be interested in purchasing that functionality to achieve the kind of costs savings that was just described by Tim.

And then we're also working with Microsoft implementing HealthVault community connect on the front end of the process to support people being able to fill out their registration forms and to track that process of, you know,
we're working with the joint center. And they
looked at the number of times that people filled
out the same form as part of this one process.
So, you know, sleep studies and those sorts of,
you know, do we need a sleep apnea study, those
sorts of things.

So we're trying to bridge the gaps
between, you know, the clinical systems, the home
system, and the processes and support those
processes. And those would be billed services.

MS. KENYON: So you've moved from
grant-funding and you're looking at a sustainable
model, and right now you're looking at mainly
providers.

MS. NICHOLS: We'd love to continue to
receive grants.

MS. KENYON: Okay.

MS. NICHOLS: But we were actually going
to be -- we just got word that we did get another
small grant that's going to facilitate working
with our local area Agency on Aging to have them
become people who can register, go out and
register their clients in the home so that there is some more ability for them to track and coordinate care.

MS. KENYON: Out of curiosity, have either employers or health plans supported you at all because of the savings they may have?

MS. NICHOLS: Those are both kind of notably absent in part because patients have said they really don't want those entities to have access to their health information. It's been one concern that we have heard. That said, we are looking at large, self-insured employers as people who actually understand what the cost is and what the cost savings could be by being more efficient in providing better care.

MS. KENYON: How do you get consumer -- consumers telling you that? Do you have them on your board or --

MS. NICHOLS: We have a Consumer Advisory Group. We do presentations. We, you know, we talk to people.

MS. KENYON: Okay.
MR. SCRIBAN: All you really have to do is show up at one of these things. You will hear that patients are most concerned when they talk about putting -- when individuals talk about putting their health information online. Their number one concern is, will this, you know, allow a plan to deny me coverage, or when I, you know, search for life insurance, when I try to get life insurance, will this become a problem? And will employers be able to deny me employment as a consequence of my health information being online.

MS. KENYON: I'm looking forward to the privacy questions that I've got coming up here. We're getting into them already.

Yeah, so tell us your -- you mean you give away your --

MR. SCRIBAN: So, we're just good guys.

MS. KENYON: -- your PHR.

MR. SCRIBAN: We're known for our generosity, I find. No, one of the reasons I mention the broader group that I work for, Microsoft Health Solutions, is that we don't view
HealthVault in isolation from the other products and the other solutions in our portfolio. We know that there are entities out there, health care providers in particular, who are very interested in actually being able to systemically improve the care that they deliver, and they're interested in a vehicle to get that, to extend the systemic improvements to the patient, literally, a vehicle that allows them to reach out to the patient and engage them in health care.

On the flipside, they also understand, like we do, that patient trust is paramount. No one's going to participate and engage in this process unless they feel that the data that they're contributing and the place where they're storing their information is trustworthy. So we had to be very, very clear that the last-mile piece of what we were doing, distinct from the enterprise solutions for which we charge, you know, directly to providers to roll out and implement, distinct from that there is this last-mile bit of infrastructure that we call
HealthVault is under the control of the patient, and we had to drop the barrier and be very clear about who our customer was, that it is a free platform that we offer to consumers in the United States that they control.

Mind you, the United States -- and I will, you know, in the interest of full disclosure -- say that I'm actually a permanent resident here. I'm a Canadian citizen, so I've seen other health care systems at work, and I also happen to have my information fragmented across borders now. But I've seen other health care systems at work, and where there are more concentrated bearers of risk in health care, it becomes a little bit easier to think about HealthVault in a, you know, from a -- or something like HealthVault as a commercial enterprise. So in countries like Canada or in Germany, HealthVault is actually licensed to a partner in Canada to talk about -- in a big health information company called Telus, to Siemens in Germany, and in countries like the U.K. Where we've launched, there are commercial
models behind it because there are very large
bearers of risk and more centralized, you know,
ways in which health care is not only delivered
but also paid for.

That doesn't exist in the United States, so the United States is a bit of a -- you know,
our chief technology officer at Health Solutions Group likes to call the U.S. our HealthVault Test Kitchen. So that's the model for HealthVault, but, really, it's driven largely by the
recognition on the part of everybody that we serve at the Health Solutions Group that it's such a
critical thing to get the patient and the consumer involved and engaged and using this, that you
cannot muddy the waters too much and appear to be, you know, really have -- your customers are really
over here in the provider plan/government employer space, but, you know, trust us. It's safe to put
your information here.

MS. KENYON: Your business model, then,
really requires that you're part of a -- of an
income, of a revenue source that's bigger than --
because you're pulling, you're basically
supporting your PHR --

MR. SCRIBAN: That's true.

MS. KENYON: -- out of other business

lines. Okay, Greg.

DR. STEINBERG: Right. So, as I said

before, our customers are health plans and large
employers, and they buy a set of services from us
that are designed to improve quality and lower
costs. The PHR is one of those services. It is
never purchased alone. We are typically paid on a
per-member-per-month basis for those services,
and, as I said, the PHR is never purchased on its
own. It is always purchased with some combination
of decision support and usually disease management
or a lifestyle management.

As we move into this world of health
information exchange and health information
technology where our customer base are now
increasingly large integrated delivery systems,
there the payers are these provider groups, the
physician, large physician groups. And the PHR is
a -- is also considered part of the suite of services that we provide to these guys in order for them to communicate bilaterally with their patients over the health information exchange. In that situation, the revenue model is a per-provider-per-month basis.

In terms of growth, we're definitely growing. We're exiting 2010 excluding, as I said, the 8 million Aetna members with about 1.9 million members on the non-Aetna PHR, and in January, in a couple of days we'll probably be up to about 2.7 million.

Just to echo what was said in terms of the use, it is our experience as well that incentives play an acute role in dictating the actual usage as well as how well or badly the tools are promoted.

Incentives are an interesting thing. Just to give you a little anecdote here, one of our large customers, it was a commercial bank, had an incentive for their employees to fill out their health risk assessment in the PHR, which was a
sort of credit card thing for about $75, and we had a tremendous rate of adoption that was good, about 75 percent. But being that it's a bank and it's a credit card, they could track where the money was spent, and the largest amount that was spent on Kentucky Fried Chicken.

MS. KENYON: Not -- not right. Yes, okay. Uh, you know, I'm going to warn a couple people in the room that I'm going give you an opportunity to ask questions as we move into the privacy section.

Dr. Blumenthal, if you have any questions that you'd like to ask, be thinking about it because I'm going -- since you've stayed, you're going to get the opportunity to ask them.

And, also, Joy, are you here? Where's Joy? Okay, I'm going to also give you that opportunity as we move into the privacy questions.

We've really laid the foundation now and actually started talking about privacy somewhat. My first question on my planned list is, how do you inform individuals about how you use and
disclose health information in the PHR? I think
I'm going to ask each of you to answer that
case, we go into -- I'm going to ask you a
specific question about your particular
organization, and again I'm going to start with
you, Colin, at Dossia, because we heard Lori say
that consumers are sometimes concerned about
employers, and we do hear that.

And so one of the things I'd like to
know is, you know, how do you inform your
individuals about how their information is going
to be used and disclosed? What, if any,
information do you give to an employer sponsors?
And how do you reassure people that their
information is private?

MR. EVANS: Well, it's, you know, I
often hear this sort of, you know, oh, my
goodness, a system provided by employers, so they
must see my data. Well, you know, we go to a lot
of trouble both in terms of our overall privacy
statement of policy, and the mechanics of people
signing up with the system make it clear this is
an independent system that is keeping your
information, you know, your supervisors from
reading this database as you put in information.

We do that through the mechanics of
people signing up. We do it through our project
statement, we do it through the way most employers
promote the system inside their companies, and in
kind of legal words -- "clear and conspicuous" I
think are the words in the law -- you know, there
are clear and conspicuous choices that people make
as they go through a role in deciding which data
sources they want to subscribe to authorizing
which applications they want to use, at a very
granular level deciding which information they
would like to share, which information they'd like
to protect or annotate. And there are a lot of
tool sites.

There's no doubt to anybody as they're
using the system this information is for them and,

you know, this is not shared information unless
they want to share it to anybody. We don't share
any information with employers other than kind of,
you know, this is how many people have signed up. That's about it. And we make it clear we don't mine the information, we don't sell it. So I think we're as clear as we can be to everybody.

MS. KENYON: Okay.

MR. EVANS: And then to some extent I think people are concerned about their employer, but, you know, for people, you know, employees of large companies, I think they understand that there's a bargain here in terms of the way they get health insurance from their employer.

MS. KENYON: Mm-hmm.

MR. EVANS: The information at Dossia is completely private, and they know that.

MS. KENYON: And you answered a question that I was going to ask later, and that has to do with, do you, as part of your business model and part of your privacy practice-- I mean, how do you handle the potential to de-identify or aggregate data and share it. And, as I understand it --

MR. EVANS: Just say no.

MS. KENYON: Okay. Greg, you kind of
had the same problem, I think, that people don't necessarily trust their health plans, they're worried about their health plan -- I shouldn't put it that way. They trust their health plans. They worry about their health plans having access to information on them.

DR. STEINBERG: Yeah. I think, actually, in our experience there is some concern about the health plan, but I think there's a sort of understanding on some level which is true that the health plan already has a lot of this data anyway--

MS. KENYON: Yeah.

DR. STEINBERG: -- so, you know, okay. I think there's more concern relative to their employers.

MS. KENYON: Okay.

DR. STEINBERG: There's more concern there, and so, you know, we go through a lot of the same hoops that I think that were pretty clearly articulated just now. We do tell them the type of data that we have access to and that we
get data from the health plans, from the PBMs, from the lab systems. Also, obviously the data that they enter, explain to them how this data might be used in terms of providing them and their physicians with the clinical decision support that will hopefully improve their health; that it is going to be shared within the other applications in our system to the extent that that's necessary like lifestyle coaching and disease management; and that it will not be shared at all with their employer other than to the limited extent that would need to happen, say, with respect to incentive management.

MS. KENYON: Okay. Lori from Shared Care Plan, do individuals who use your services, do they -- you clearly have a connection with Microsoft HealthVault.

MS. NICHOLS: Mm-hmm.

MS. KENYON: And so is there -- do you go from an entity that is, you know, sharing that's within a covered entity under HIPAA and then over to Microsoft HealthVault? Do people
understand that transition and how are the privacy practices different?

MS. NICHOLS: They are presented with both privacy policies. As part of signing up, they sign up for a Shared Care Plan account, and that also then has them create a HealthVault account. They're presented with and have to, you know, acknowledge both privacy policies.

We have an online tutorial, online description that talks about that, the brochure. We have live people who answer the phone, but I think the key thing is one thing I think we do that's a little bit different than other folks is that we show the audit trail to the consumer, so as to see --

MS. KENYON: Explain that one.

MS. NICHOLS: You can see who has access to your plan. You know, obviously we don't have the same concerns, you know, live concerns about addressing access by insurance companies. The question comes up and we address it. But people can see who has accessed their plan, and more
often than not they see who hasn't accessed their plan because usually they're the only ones that are accessing it. And they can also see for any item that gets changed in their Shared Care Plan. If they've granted someone else access to it, they can see if that item is flagged as having been changed since the last time they logged on.

And that's true for both the individual -- that's true for anyone who logs into anyone's Shared Care Plan, if they have the authority to do so.

MS. KENYON: I'm going to give George an opportunity to speak to this, but are you pretty much in the same boat with Dossia and Greg with Aetna, ActiveHealth?

MR. SCRIBAN: You know, to an extent. It's a little clearer for us simply because we, you know, we are quite -- we are one of those, the services where a consumer can just dial up, www.HealthVault.com, and sign up for an account. So, you know, if that's the way that they initiate their relationship, there is sort of an
expectation set up that, you know, that this is a service that is a contract between them and Microsoft to collect, store, and share their personal health information. So they, you know, the expectation is set up slightly differently.

The defining, you know, kind of the core principles upon which -- we boil down our privacy practices to four central principles, and then articulated them thus: The record that you create in HealthVault is yours, you control it. You own it. Nothing goes into that record without your explicit consent and action, nothing leaves that record or is used by anybody in that record without your explicit action and consent.

And the fourth one is that Microsoft won't make use of any of that information, not to target advertising, not to customize your experience, not to market to you unless we explicitly ask and you explicitly give us permission.

The whole point is to engender trust, and trust is really rooted from the consumer
standpoint in control, in transparency, and in security. So the, you know, some of the stuff, some of the things that we do in terms of giving consumers control of their health information include allowing them to choose what credential they're going to use to secure their HealthVault information. They have the option of Windows Live Art using the Windows Live ID, for example, or using an open ID with a, you know, with a second factor.

They get to control, of course, what sources of data they connect to, and, obviously, they can, when they connect to a source of data or when they connect to a third-party service -- let's take the American Heart Association again -- each one of those services has to be very explicit about exactly which types of information they're going to have access to in a HealthVault record, and what they're going to do with that information.

MS. KENYON: I am concerned about those transitions between your set of privacy
principles, and I'm interested in this for others as well, and when you're basically linking to a different entity, how is it that individuals would know they're moving between privacy practices? And do they really understand it?

MR. SCRIBAN: It's an interesting question, and there is a whole body of scholarship around choice, notice, consent, do people read privacy policies, do they understand what they are seeing. I think to a large degree, I think what, you know, anecdotally what a lot of researchers showed is that the existence of that little privacy link at the foot of the web page for most people means that their privacy is protected. Is that sufficient?

We try to make the decision an informed one. We control that experience. We're not an open platform. It's not Facebook. It's not like any third party can deliver a HealthVault application and, you know, we don't know about it. So we do try to constrain the degrees of freedom our third parties have.
So when, for example, I, say I would like to use Heart 360, when I go through the process, say I'm on the American Heart Association site and I think this is a very interesting looking application, and, you know, I would like to use this. And I -- so, you know, I just happen to have a HealthVault account where I have data. So I realize, you know, this is a HealthVault-compatible application. The experience of authorizing that application, to have access to my HealthVault record is controlled by HealthVault. I go literally from Heart360.org to HealthVault.com to sign into my account to where the platform steps the user through the processing: This application wants access to one of the records in your HealthVault account. Which one of them do you want granted access to?

Because, say, for example, I would have -- I could have my record, and, you know, those are my children and that of my spouse in my account. Then the next step is: This application wants to have access to your blood pressure
measurements, your medication list, your condition list, your allergies, maybe a few other data types. Out of the 80-some data types that we store, we require our third parties to be explicit about which subset they're going to have access to and what they're going to do with it. They're just going to read it? They're going to be able to augment that data, append data to it? That kind of thing.

They also have to present their privacy policy for that particular application, including what they're going to do with that data, if they have read-access, for example, to that information, and their terms of service. And I get to see all of this in an explanation, data type by data type, as to why before I click -- before I give them my consent, before I say: I authorize this application. We handle all of that, and that's one of the technical measures of control that we put in the hands of users. And then we back that up by embedding within HealthVault itself a granular -- and by "granular"
I mean right down to the individual data element -- so to every, like, right down to an individual blood pressure measurement and audit trail that is immutable.

So you can tell what applications have access or what other people have access to a data type, and then you can watch the history of the specific piece of data: This blood pressure measurement was written by this application at this time; it was modified by this application, and so on and so forth.

MS. KENYON: Okay. Colin, you wanted to say something about Dossia.

MR. EVANS: No, I just wanted from an architectural perspective, I think we're, you know, similar in the same boat that the HealthVault is in terms of the way we look at things.

MS. KENYON: Yeah.

MR. EVANS: But when I listen to this discussion, it feels like we're looking through the looking glass the wrong way. I mean, people's
information for the most part, I think for most of
the panelists, you'll see here goes from a world
that is totally incomprehensible to most consumers
about where the -- and totally invisible and
opaque -- where is my data? Who is using it?
What are they using it for? You have no idea.
Your data then goes to a place where you have very
explicit, very clear, very granular control. You
know exactly what's going on.
I think, you know, when we look at this
whole privacy debate, we're looking at the
telescope the wrong way. I mean we're sort of
looking at these systems, in some sense, as being
very over-engineered for the level of control
that's needed legally, in order to establish the
kind of credibility and trust that George is
talking about, from a system where you have no
idea what's happening to your data. I think we're
sort of looking at the world a little bit the
wrong way.

MS. KENYON: You know, it's interesting
because, you know, I come at this as a lawyer, and
one of the --

MR. EVANS: Don't we all?

MS. KENYON: -- and so, Tim, you know,

we know that Tim is, his PHR is under HIPAA.

MR. EVANS: Yes.

MS. KENYON: We know the privacy

protections there. What I'm hearing from both

Colin at Dossia and, you know, George at Microsoft

HealthVault, and I assume Greg, is that even for

your PHRs that are not subject to HIPAA

protections, that you have -- you're quite

convinced that it actually gives individuals more

control. Am I hearing that with their privacy?

MR. SCRIBAN: Well, I mean --

MS. KENYON: Though you don't have, as I

understand it, you don't have explicit legal -- I

mean your controls are contractual, am I correct,
on privacy?

MR. SCRIBAN: Our controls are

contractual. Our controls are governed under, you

know, you know, unfair and deceptive trade

practices under the FTC. I mean we have that,
that kind of implicit contract with the end user as well.

You know, I get questions from individual users. I tend to respond to them. They get forwarded to me, and quite a few of them come to me asking, is this service covered under HIPAA? Is HealthVault a HIPAA-covered service? And I -- sometimes I feel like responding by saying, you realize the P in HIPAA doesn't stand for privacy, right?

The -- and there's -- although it might not be -- we have a saying at Microsoft, we use a phrase called "the rathole." We might not want to go down the rathole as to what privacy protections are and aren't covered under HIPAA, and whether HIPAA is sufficient as a consumer privacy protection law, which I think a lot of patients believe it is, but we don't have -- we don't -- we explicitly close off loopholes, Dossia and ourselves, at this table. We don't permit secondary use of information or onward transfer. There is no payment, treatment, or operations
mechanism for us to do something else with your information that you don't explicitly consent to. We have to earn the trust of our users and keep it by being very clear about what's going on. It's not the same as E-prescribing, and all of the different players in the information supply chain who probably do legitimately require access to this information in order to make a simple prescription written on a pad over here wind up in a bottle of pills in my hands over there.

MS. KENYON: Okay. You know, because we end it, I want to make certain that if, Dr. Blumenthal, do you have a question you'd like to ask, and if you do you're going to have to come up and use the speaker, I'm afraid.

DR. BLUMENTHAL: I'm sorry, I'll pass.

MS. KENYON: You're -- okay, Dr. Blumenthal's going to pass.

Joy, I'm going to let you ask some questions here.

MS. PRITTS: I can never -- I'm sorry,
but I used to be a trial attorney, so I can never
pass up the opportunity.

MR. EVANS: I put it to you --

MS. PRITTS: Is it true, as we start,

yeah I won't do that...

MR. SCRIBAN: Yes or no, Mr. Evans? Yes

or no?

MS. PRITTS: When did you stop beating
your wife? Okay, my first question is kind of
along the lines of the one that Kathy was just
asking, and this is for Colin. I believe that you
said that you believed that a lot of your
programs, because of the way you interact with the
employers is usually through the employers' health
plan, that you are HIPAA-covered or a business
associate, but in actuality what I believe you
said was, that you go beyond what is required by
the Privacy Rule and in your assurances that you
make to individuals about how their information is
handled. Is that accurate?

MR. EVANS: Yeah, I think so. And I'd

kind of go along with the stuff that George is
saying, in terms of the level of control and
clarity that we provide to individuals when about
the way they manage information, yeah.

But I also think, it's not -- there's no
such thing as a sort of certifiable system under
HIPAA. I mean there's the CCHIT for certifying
EMRs, but there's no sort of official stamp of
approval that says you've got HIPAA certification.
I mean, we subject ourselves to audit that way.
Our (inaudible) audit and our financial auditors,
inspect us from a HIPAA perspective, but there's
no sort of clear, you know, label that says where
you are and are not relative to HIPAA.

MS. PRITTS: Okay. Since I have you on
the stand, is Dossia interoperable with other,
like, HealthVault or Google, or any of the other
--

MR. EVANS: Individuals can offload
their information not just in a PDF but in a
computable form to transfer somewhere else if they
want to. But, you know, we haven't had many
people want to do that yet.
MS. PRITTS: Okay. My next question is a more general question. In my limited understanding of the huge Health Care Reform Bill, I understand that employee assistance programs are going to be playing a more central role and that there are more incentives for individuals to meet certain health goals and more penalties if they don't in the way that the insurance is evolving; that employers will be able to charge them higher premiums if they don't meet certain goals. And it's increased quite a bit from what it used to be prior to Health Care Reform.

Do you see these PHRs and technology being used to implement that part of Health Care Reform? And I'll toss that to anybody at the table.

DR. STEINBERG: Yeah. I mean, the short answer is I think it probably will. I think, clearly, it's going to be problematic to figure out exactly what kind of information could and should be shared in order to effectuate that. But in terms of having the underlying tools and
capabilities to monitor that, that's fundamentally exactly what, at least at our end, what we have.

And when we - as I mentioned we have these very clearly-defined, prioritized, clinically-intelligent health actions, if you will, that are dynamically adjusted as an individual goes through and sort of checks off that they have done or have not done whatever it is that's being suggested and provides them with a score and an output on that, and to the extent that those may be tied to various kinds of negative and/or positive incentives, you know, it's the carrot, the stick, and then the frozen carrot. You know, there's clearly the mechanism to tie those two together.

MS. PRITTS: Do you see this as potential incentive, or, you know, like a real incentive for people moving more towards this kind of technology? Do you think this is going to be one of the big factors going forward?

DR. STEINBERG: Uh, it already kind of is. So, as I mentioned, you know, the positive
incentives have clearly -- and I think this has
been echoed, I mean to the extent that you provide
incentives for people to use these tools -- they
do. And it's actually sort of interesting how
relatively meager it is these incentives have to
be in order to significantly move the dial in
terms of usage.

MR. SCRIBAN: Although while I agree, I
think that's sort of just one component of it.
Our experience kind of -- our experience indicates
that the number one factor, not necessarily an
uptake -- and I believe incentives can really help
drive initial adoption -- but ongoing engagement
and use, ultimately that utility really only is
maximized when more of your primary care tier is
digital. And right now that's kind of the big
gap, right. If all of our care was delivered, you
know, through integrated delivery networks or
through at the acute care level, it would be easy
to get your digital records.

But for most people the part where it
drops off in terms of utility is not having your
pediatrician, your gynecologist, your family
doctor, you know, using an electronic medical
record so that you can't actually meaningfully
come to them except with stuff on paper out of
your HealthVault record, out of your Google Health
record, out of Dossia record, or, you know, with
information from your other providers and present
sort of like a coordinated, you know, family
health or personal health history in front of your
physicians.

DR. STEINBERG: And I would completely
agree with that, but I would add even one further
layer, which is moving information around the
health care system is tremendous. Providing
individuals with actionable information is better.

MR. SCRIBAN: Yep.

MS. NICHOLS: Yes.

MR. EVANS: Agreed.

MS. PRITTS: I think we're unanimous on
that point, aren't we?

MS. NICHOLS: Yeah. The only other
thing I think I would add is that it has to be
easy and -- I'll say it, sexy. I mean it's got to be --

MS. PRITTS: Fun.

MS. NICHOLS: -- people have -- yeah, it's got to be fun, people have to want to use it, it has to be convenient. So I think, you know, as we move, you know, more to the SmartPhone accessible applications, we're going to be reaching the audience that we have a chance to keep healthier, because some of the people who need PHRs the most right now and who actually get it are not the highest users of technology. But they can be supported, and that's, you know, we're going to be doing a project with our area Agency on Aging to help support people who need help with the computer part of it.

But it's, you know, it's a continuum.

MS. PRITTS: Okay. I'd like to go back. I had another question here about - Oh, did you want to go?

MS. KENYON: I just have a couple more questions, not yet.
MS. PRITTS: Oh, I'm sorry. I'm just hogging the mic here. Look, you know, the incentives to sign up for PHRs -- I found your story entertaining, but also I was sitting here thinking about it. So we're going to have more incentives to sign up for a PHR or to record your health information in order to tie that to your premiums and then the employer health care setting.

So is there any incentive for anybody to actually verify that the information that the patient has entered into their system is accurate?

DR. STEINBERG: Hmm. Not yet that I'm aware of anyways. We also have, you know, increasingly -- we haven't really had a lot of experience in dealing with it for real, but, hypothetically, clearly, there's, you know, we're getting, for example, medication information. So we get it from the PBMs, we get it from the patient which one's the right one. Is it both? Right, so these are the -- particularly, and it's particularly important for us, because we
use that information not just in a passive way to sort of put it somewhere for somebody, for an individual to see it, but we are using that information to run up against decision support roles, that then spits out information that goes back to the physician and the patient saying, you know, based on the information we've been given, you should do X, Y, and Z, or should at least consider it. So it becomes a potential conflict. Now, so far we've not experienced that conflict in reality yet that I'm aware of, but I suspect it's coming.

MS. PRITTIS: Lori?

MS. NICHOLS: We have, and I think there's a fallacy that somewhere in existence there's a single accurate medication list.

DR. STEINBERG: Mm-hmm.

MS. NICHOLS: It's a series of conversations. Just because something's been prescribed doesn't mean it's been filled, doesn't mean it's being taken the way it was prescribed.

DR. STEINBERG: Right.
MS. PRITTS: Doesn't mean they didn't get their friend's meds.

DR. STEINBERG: Right.

MS. NICHOLS: And people share. We actually did have some experience and did study as part of an AHRQ grant where we built our medication reconciliation function in the Shared Care Plan that they were using an electronic medical record. They had the meds. The patient's list was more accurate, and this was stated by a pharmacist that -- because the patients know what they're taking.

MS. KENYON: Joy, are you --

MS. PRITTS: Okay, I had a few more -- I'm going to change, shift the topic because I have a whole list of questions here now -- to I wanted to ask a little bit more about the notices that people were explaining. Do you -- does anybody, when you're posting your privacy notices or you're trying to explain to individuals how their information is to be shared, can you explain to me your process for developing those? Do you
have literacy specialists involved? Do you consult with consumers? How does that process take place? And again I will throw it out on the table for anybody to answer.

DR. McKay: It's really layered, so our privacy has been noted already. We're really under our notice of privacy practices. As a company, though, we have eight different notices of privacy practices which are largely the same, have some state variation in them that we have to account for.

We have another layer under that with our web privacy practices which is, it's compliant with the notice but goes into specific practices like the use of web beacons, the use of cookies, et cetera.

And then we have a third layer which is terms of service. So in the particular services we offer, then how is that information specifically used and disclosed?

One thing that we -- and also it's been noted -- is very, very few people read those
statements. When we look at counts of the numbers
of people who actually go to the privacy notices,
it's minuscule.

So we made a decision in --

MS. PRITTS: Can I interrupt you? You
have those counts? Can I get those from you --
not right now, but --

DR. McKAY: Possibly, yeah. Let's talk.

MS. PRITTS: Yes, let's talk because
that's very interesting information for us to
know.

DR. McKAY: Oh, but one thing that we
decided to do with our site redesign was to look
at when we present our terms of service, could we
take out and bullet out the concerns that people
mostly have so, especially with third-party
sharing of information we just don't do it, but to
state that up front to give what the salient
points are, and then give people the opportunity
to read the full notice we found it actually
improved people's understanding of what our
privacy practices were.
We have a general principle with everything we do on the site is we usability test, and test and test and test until things are understood and usable by our population. In particular, our average intake is about --

MS. PRITTS: Can I, can I --

DR. McKAY: Sure.

MS. PRITTS: -- when you say you usability test, do you do that with your actual members?

DR. McKAY: We do it with members and nonmembers.

MS. PRITTS: Okay.

DR. McKAY: So it's a pretty well-designed process. It follows a lot of normal industry standards. But we do usability testing in conjunction with rapid prototyping, so we bring in actual prototypes of the services that we expect to use, do rounds of testing. We'll go back and make prototype changes, do additional rounds of testing until we get a usability score for our population that is high enough for us to
launch the service.

MS. PRITTS: Anybody else want to -- do you do any testing:

MR. EVANS: We've done quite a lot of work to try and distill a privacy policy and practice to -- as simple a policy it can possibly be. We send out eight different ways of doing it, but I have had some quarters when I've spent more money on lawyers than developers, and some of them in this room -- lawyers, that is.

But, you know, I think this discussion just sort of reinforces to me the kind of thing that keeps coming back to me which is that, you know, individuals understand medicine; they just don't understand health care, right? And all of this kind of stuff is just getting in the way of people actually connecting to their doctor and their data. And I think a lot of these layers and layers and layers of stuff, unless we figure out to simplify it, will prevent people from feeling like any enthusiasm for getting involved in their own health because this is just too confusing for
people, really.

MS. PRITTS: Mm-hmm.

MR. EVANS: We've got to keep it simple.

DR. McKAY: There was a small study that we did last year that looked at the idea of how does trust in brand trust move over into perceptions of privacy and security. And what we found, at least for our population, is that they're very highly correlated so that if you have trust in the organization, and our members have had trust over the years, with how we deal with health information, that that trust is also translated over to the web.

MS. PRITTS: Can I ask if any of you provide your privacy notices or other materials like that in languages other than English?

DR. STEINBERG: Spanish.

DR. McKAY: Spanish. And Chinese, I believe. Mandarin and -- it's escaping me, yes.

MS. PRITTS: Kathy, I'm going to turn it back over to you. Thank you very much.

MR. EVANS: A pleasure. A pleasure, Your
(Laughter)

MS. KENYON: Well, my questions are not as much fun. I should give -- we have until 10:40. I have one question that I'm going to ask which I hope will be quick, and then if there are questions that panelists have of each other, I'm going to give you a couple seconds at the very end to ask that.

I'm just going to skip the questions on security, we're going to run out of time for that. My question has to do with the National Committee on Vital Health Statistics, has recently urged the development of the capacity to allow more data segmentation, meaning the ability to allow individuals to mask information that's more sensitive. I think we've heard from Microsoft HealthVault that you do that, but I'd like to hear from some of the others about whether this is an issue that you hear from people that they want that ability, and are you providing it?

Why don't we -- well, let's start with
DR. McKay: In a shared record, masking is basically impossible so that, because we're drawing off the same data sources. What we do, though, in terms of internal controls are using role-based access to the records so that people should only have access to the information that they need to do their job. And so we rely on that mechanism, we rely on audit to make sure that the controls are in place.

Now, the question is when you send something out, then as an organization like Kaiser Permanente what do we do with vetting? So if it's to, say the information is from our source, at what point when a person starts to redacting the record do we withdraw that vetting and say it's unacceptable? You can't rely on us as the authoritative source.

Or what we've heard in working with standards groups is that the tension is with physician adoption and redaction. In practice, people redact all the time. They just do it
orally. But when something is on paper, it gives
the appearance of being more authoritative than a
verbal source. And I think we're going to have to
find that balance as an industry of the point of
comfort with where providers are willing to accept
the information and to use it, and to realize it's
just a different form of the game that's been
played for years and years and years.

MS. KENYON: Okay. Anybody else on data
segmentation?

MS. NICHOLS: We allow, you know, a very
granular level of, you know, item-level detail. I
can block one med from one member of my care team.

MS. KENYON: Wow.

MS. NICHOLS: But I think what I was
hearing you describe was something more in terms
of having standards or creating standards to
generalize "I want my mental health issues
private," and you could have some sort of a break-
the-glass access to it.

We also use role-based access as we
grant Shared Care Plan within the application.
But I think it would be useful to have those kinds of categories and linking because I think one of the dangers, if people are marking information as private, they may not go all the way through to link the medication to the lab test to the diagnosis. And if people truly want to be able to mark something as private, it would be wonderful to have some mechanism or standards that would do that and be able to be applied.

DR. McKay: I've got to say that that would be wonderful of -- we run into this problem with parent access to teen records. And we're given -- given that every single state has different rules of what kids can consent to, what they can't, the age that parents have full control of the record to when they don't -- to case law that says the older that the child gets the more they should be able to consent for their own care, and that that happens as a conversation, between the provider and the patient, how in the world do you operationalize that electronically.

And it makes it very difficult to tell a
parent, "because we can't automate this, we can't provide it to you through this channel." You can get the information by asking for a copy of the record. But it is very problematic.

DR. STEINBERG: So we -- our customers actually have asked us pretty uniformly until now with one exception I'll get to in a minute to actually filter out certain types of conditions, particularly HIV, mental health, substance abuse, from the records that are viewable by the members.

MS. KENYON: So it's not in your PHR at all?

DR. STEINBERG: It's not in the PHR. Now, that said, that has changed, and we have the ability to do that in yes or no on a customer-specific basis. Increasingly, we recently have this situation with one of our new health information exchange partners in Brooklyn where what we're doing with them is specifically revolving around HIV and mental health. So, by definition, we are having to include those diagnoses in the personal health record. So that
seems to be an evolving thing.

And the other thing I would say, though, you know, sort of the flipside of this, and, you know, about what data is viewable, you have to be a little sometimes careful. One is the thing is to provide the information, at least on a diagnostic side, in consumer-friendly terms. I mean a lot of the ICD-9 diagnostic terminology, unless you're a physician or, you know, a health care provider, is completely incoherent and difficult to understand if not outright terrifying. So you've had all sorts of anecdotal issues where people have said I didn't know I had a brain tumor, right. So you need to be careful of that.

And one of the ways, for example, we get around that is we provide the granular detail that's there in patient-friendly terms, but, in addition, we have a section where we present individuals with their diagnosed conditions, their actual conditions that have undergone some level of clinically intelligent analysis and say, well,
you may have all these ICD-9 codes over here, but
here is a subset of validated conditions that you
actually have.

DR. McKAY: At Kaiser Permanente we took
actually the opposite approach, and it was again
based on feedback that we got from our members,
which was that they wanted to see the terms that
their doctors were seeing and for two reasons:
One is that they didn't want to be talked down to;
and they also wanted the ability to take those
terms to be able to search more broadly on the
Internet for health information.

So what we do instead is we present the
terms. There are some things: like, that, with,
et cetera, et cetera, et cetera, that get dropped
-- but then we link that information to our health
and drug encyclopedia so that people can read
about the conditions themselves.

MS. NICHOLS: Yeah, we do something
similar. We have a link to a health-fit knowledge
database, but I can't agree more that patients are
surprisingly competent, and they don't need to be
shielded from actual information.

   DR. STEINBERG: Yeah. And again, I think, you know, all the data is there. It's just if you've read what it looks like in, you know, these long diagnostic categories, as you said you even, you know, chopping it up already. So it's a matter of just putting them into something that is understandable, and all those links are there as well.

   So I think we're actually agreeing, vehemently, rather than disagreeing.

   MS. KENYON: Okay. Do you have -- do any of you have a question that you'd like to answer or that you'd like to ask to somebody else?

   MR. EVANS: I can answer.

   MS. KENYON: Okay, let's start with Lori. No, that's not --

   MS. NICHOLS: Don't start with me.

   MS. KENYON: Don't start with you, okay.

   Tim?

   DR. McKAY: With one of the questions that we were presented with, I thought, was,
really interesting, with where do we see the
security and privacy challenges that are on the
horizon?

MS. KENYON: Okay. Let me ask you that
one: Where do you see? (Laughter)

DR. McKAY: In places that are maybe a
little different than you would think, we
perpetually have to enforce secure coding
practices, that there are certain things that you
just should not do when you're coding an Internet
application that you need to train your developers
in well. Otherwise you start opening security
holes.

Another would be the need to do greater
and greater in-depth testing, especially due to
browser proliferation, so all browsers do not
behave the same, and we need to test against
multiple versions of Internet Explorer, Firefox,
Chrome, and Safari as a matter of course.

The more complex that the systems get,
the more time, relative time that needs to be
spent and money needs to be given to testing in
relation to the amount of development that you're doing. And being able to maintain innovation while increasing complexity, I think is one of those challenges that we're going to have to find a happy medium.

MS. KENYON: Okay. Let me ask a security challenges from Colin Evans, Dossia, because I know that's in your background.

MR. EVANS: You know, we don't -- I mean, technologically, I don't think we've come across anything that's particularly difficult. Frankly, when I was looking at that question, the one area that came, that struck me most when I was sort of thinking about it, was the apparent difficulty most of the rest of the industry has in passing secure data.

We had one large health plan that will remain nameless, you know, wanted to send us data on a CD, or their IT people didn't want to send secure FTP. I mean, there were a lot of issues where we were trying to get basic things in place that I thought were pretty routine industry
standard, normal ways of transmitting data. And we've -- now that may just be because they were throwing logs on the railroad because they didn't want to send the data. But, you know, some of the difficulty we had is actually in some of those external connections. We think there are pretty well-formed industry-recognized practices for secure data transfer that many people don't seem to know how to use.

MS. KENYON: That's interesting. So it's the human factor.

MR. EVANS: I could never figure out whether it was really they did have incompetent security people or they just didn't want to send us the data. And right now, you know, the jury's still out.

MS. KENYON: So it the major security issue is incompetent security people, so -- Greg?

On security challenges.

DR. STEINBERG: Yeah. I mean I think that from our perspective what's been sort of interesting, we have -- like I'm sure everyone
else here, I mean, we have from an architectural perspective, I think, you know, we have security around our presentation layer, our application layer, our basic database layer. And we have all sorts of internal and external audits that are performed, ethical hacks -- which is a sort of interestingly oxymoronic term -- that occur. So, you know, and to my knowledge these have always been fine.

MS. KENYON: Have you had security breaches?

DR. STEINBERG: No. No.

MS. KENYON: Okay. And George:

MR. SCRIBAN: Are you asking me if we've had security breaches?

MS. KENYON: Well, you know, I -- you will be free to answer that question, but I'm asking you for security challenges.

MR. SCRIBAN: Security, well, I think you're going to get a very different answer from the technology-centric companies here than the health care-oriented entities. You know, we have
a reasonably long tradition and, in fact, have
kind of established that the industry standard
around secure development practices with the
security development lifecycle at Microsoft, which
is not proprietary to us but something that we
share with the rest of the industry.

So, you know, it's ingrained to us to
bake security into the development lifecycle, to
bake privacy concerns into the development
lifecycle of all the products that we release. So
as to, you know, specific security concerns around
data interchange, I think, you know, my experience
is a lot like, like Dossia's and Colin's to the
extent that, you know, not us; some of our
partners may have an interesting -- it's
interesting doing engagements with partners.

And I think there's the other thing that
I find myself constantly coming up against is when
we deal with third parties' data sources,
community hospitals, or health care providers, or
payers or PBMs who want to deal with, who want to
enable their patients or members to pull a copy of
the record into HealthVault, the information-risk people on the traditional health care entity side looking at us and trying to figure out, okay, so how do you guys fit into HIPAA? I want to know, do you comply with HIPAA? So we're constantly being asked questions in terms of information, governance risk, security questions, always through the lens of the HIPAA Security Rule and the HIPAA Privacy Rule.

I'm not saying it doesn't apply. And, in fact, we've gone out and we've been accredited as a HIPAA Security-covered entity by URAC just to show, you know, our good faith in our practices and to try and make it translatable and relatable. But we've got this -- it's almost like an impedance mismatch. I've got a situation where the rest of the health care ecosystem speaks, thinks, lives, breathes HIPAA, and it's various strengthenings and modifications, and we're outside of that realm. We talk possibly, you know, in terms of different information security and privacy frameworks, and the twain are having a
hard time meeting. They meet in me.

MS. KENYON: Well, you know, I think --

MR. SCRIBAN: And we are filling out forms --

MS. KENYON: -- we're going to get to pick this one up, especially in Panel 4.

Thank you very much. This has been a fascinating --

MS. NICHOLS: (inaudible)

MS. KENYON: I'm over. I'm into the next panel, I am sorry, Lori.

Okay, thank you very much.

MS. NICHOLS: These are experienced challenges.

(Applause)

MS. KENYON: Yeah.

MS. PRITTS: We're going to take a quick five-minute break while we set up for the next panel.

(Recess)

MS. PRITTS: If we could please get people to take their seats, we can start with the
next panel. For people who do not take their seats, I'm going to start singing and you will all regret it. We have bouncers. See, that got everybody's attention. Okay, please take your seats so we can start with our next panel.

For our next panel, we will be discussing new forms, new audiences and new challenges. And we heard a little bit of new challenges in our last panel, but this is just going to expand our horizons even more. It's going to be a very interesting panel, just like our first one, and I'm really psyched about hearing what is going to be said on this one, because I know some of the things that are in this panel, and it's some really cool stuff.

So to moderate this panel, we have a really cool person from ONC, Wil Yu, who is a Special Assistant of Innovation and Research for us. He leads innovation efforts of ONC, he's a Senior Project Officer for the Strategic Health IT Advanced Research Projects, many of you have heard this referred to as SHARP. And this project funds
research on achieving breakthrough advances to
dress some of the barriers that have impeded the
adoption of health IT, including some in security,
patient-centered cognitive support, secondary use,
and applications and architecture. So I will turn
these proceedings over into the capable hands of
Wil Yu. Thank you.

MR. YU: Thank you, Joy, a lovely
introduction. Thank you all for joining me today.
It's very exciting to be here, and it's wonderful
to see so many eager and enthusiastic faces in the
audience.

We have a very distinguished group of
individuals today to speak a little bit about the
evolution of PHRs and related technologies. We
hope to cover a diverse set of issues regarding I
guess different communication channels, different
organizational and business models, as well as the
various types of audiences that are being
connected to digital health and their own consumer
health data.

So let me first start off with a brief
introduction of the panelists. Immediately to my
left I have Steve Downs. Steve Downs is Assistant
Vice President of the Health Group of the Robert
Wood Johnson Foundation. His responsibilities
include serving as a member of the RWJF Pioneer
Portfolio Team, which seeks innovative projects
that catalyze fundamental breakthroughs in health
and health care. He works with program staff to
achieve the Foundation's goals in reversing the
epidemic of childhood obesity, driving fundamental
improvements in the nation's public health system,
and addressing the needs of vulnerable
populations.

Mr. Downs and Foundation staff are
developing programs to expand health information
technologies that can dramatically improve the
quality of American health care. So welcome,
Steve.

MR. DOWNS: Thank you.

MR. YU: I'd like to introduce Darcy
Gruttadaro. Darcy is the Director of the National
Alliance on Mental Illness and Child and
Adolescent Action Center. She recently played an instrumental role in developing StrengthofUs.org, which she'll be describing in a little bit, NAMI's online resource center and social networking website for young adults living with mental health conditions.

Before joining NAMI, Ms. Gruttadaro worked as an independent legal adviser and policy analyst for the American Managed Behavioral Healthcare Association and other health care and advocacy organizations. So welcome, Darcy.

MS. GRUTTADARO: Thank you.

MR. YU: To Darcy's left we have John Moore of Chilmark Research. John has been an IT industry analyst for more than 15 years, predominantly in the manufacturing sector. But in 2007, founded an analyst firm, Chilmark Research, to apply his research expertise and knowledge in the health IT market sector.

A core focus for Chilmark is adoption trends and use of consumer focused health IT solutions including PHRs. And he puts out a
regular blog on the space and industry which I encourage you all to visit to continue to read his thoughts on the space. So welcome, John.

MR. MOORE: Thank you, Wil.

MR. YU: To his left, Gail Nunlee-Bland, Director of the Diabetes Treatment Center at Howard University, Interim Chief of Endocrinology, and Director of the Center at Howard. She is an associate professor of pediatrics and medicine and is a graduate of Howard University for the class of 1980.

Dr. Nunlee-Bland is focused on improving access to quality diabetes care, and this passion has been born out through the Diabetes Treatment Center, which is a resource for patients and practitioners to have access to the expertise of nutritionists, diabetes educators, podiatrists and diabetes specialists. So welcome, Gail.

DR. NUNLEE-BLAND: Thank you.

MR. YU: And finally, but not least, we have Doug Trauner. Doug is the founder of Health Analytic Services, Inc., and in 2007, launched
TheCarrot.com, in 2008, to provide consumers with mobile and online health programs that allow them to better engage with and manage their health and wellness.

Previously he co-founded PM Squared, Inc., a health information company that was acquired by United Health Care. TheCarrot.com, however, offers health programs for individuals, employers and health plans, and its unique approach allows users to monitor more than 15 different health activities and conditions such as nutrition, exercise, medications, moods, symptoms, et cetera. So welcome, Doug. We look forward to your perspective courtesy of TheCarrot.com.

MR. TRAUNER: Thank you.

MR. YU: As you can see, we have I guess a diverse set of backgrounds joining us today, some from a 30,000 macro perspective on the consumer health data space and some that are actively part of organizations that are in the trenches trying to better understand and develop a sustainable model for success. And it's my hope
that we can learn from both those perspectives as
people begin to discuss what the future of the
space looks like.

So the first open ended question that
I'd like to throw out to the group is, please,
each of you begin to talk a little bit about your
organization, I guess how you play within the
ecosystem, and really a kind of macro-level
perspective on what the next three- to five-year
holds. We'll begin to drill down and try to have
a lively, interactive discussion following this
set of answers. So, Steve, why don't I throw it
out to you first.

MR. DOWNS: Sure, thank you, Wil. So
I'm thinking back to how I got started in working
around I guess what I would call consumer health
IT for the Robert Wood Johnson Foundation, and it
goes back to when I first started, and I had a
conversation with our CEO, Risa Lavizzo-Mourey,
and she said one of the trends that was starting
to give her some discomfort was that we were going
to increasingly place a burden on consumers and
patients to manage their finances, to manage their
care, to be able to sort of, you know, if you
thought about consumer-to-find health care, they
were starting to put more financial risk
associated with their health care, and she said
I'm not sure they're going to have the tools to do
that, and so it's something that we have to really
think about, is how might they be better equipped
to handle that responsibility that is increasing.

And so that started a number of ventures
for us, but I think most of my remarks and
discussion today is going to come from the
perspective of a few projects that I'm currently
involved with.

The first is a program called Project
HealthDesign, and this is a program we launched,
it's now four-and-a-half years ago, and we
launched it with the purpose of how do you -- how
can we re-envision personal health records and
take them more from the type of PHR that was being
discussed and operated a lot at the time, which
was really focused on the idea of enabling
patients to view their medical data, to go online
and see their record, see their lab results, and
really push it much more to what do you do with
that data, and make it much more actionable as was
discussed in the last panel, and really focus on
the apps. So that's a program that we created
four-and-a-half years ago. And I should also give
a nod to Doug, who is actually partnered with one
of our current grantees on that.

The second program is one -- it's a
large study we're doing right now, sponsoring
right now called Open Notes, and this is a program
that tests what happens if physician notes are
made available to their patients in a quick, easy,
electronic way.

So you all technically have the right to
go and ask your physician for your full medical
record, and we all know how easy that is to do and
how smoothly that usually goes. But in this
study, what's going to happen is, you go to see
your doctor, and at the end of, you know, maybe
end of the day, early the next day when they
finish signing their note about you, you get a
security e-mail that says your physician's note is
ready for your review, click here to see it, and
if you have any questions, click there to email
your physician.

Some physicians think this will end
medicine as we know it, and some say, well, you
know, this is kind of the way the world is
starting to work, we might as well get used to it.
But this is something we're going to study. We've
got 100 doctors, probably about 25,000 patients
who are going to be going through this, and I
think we're going to learn a lot from it.

The third sort of project initiative
activity I'm going to talk about is the Blue
Button Initiative. And I cannot claim a whole lot
of involvement in this other than we co-sponsored
a Health 2.0 developer challenger of the Markle
Foundation, and in general, I'm trying to play a
cheerleader role, and I'm doing that because I
think it is actually critically important to
innovation, and I think it's actually
1 fundamentally important to the discussion we're
2 having today about privacy.
3
4 But I want to tee up sort of three
5 themes that I hope we can discuss in some depth
6 that come from those projects, and I think these
7 have been alluded to in the first panel, but I
8 want to sort of lay them out sharply. One has to
9 do with separating the apps from the data.
10
11 And again, typically we think of PHRs as
12 having your medical record and then a number of
13 features that help with display, interpretations
14 and transactions wrapped around them. But more
15 and more we're starting to see with services like
16 HealthVault that the data live over here, and then
17 there are lots of apps in other places that draw
18 on those data. And there's some interesting
19 discussions about that, whether it's important to
20 have platforms like HealthVault. Matthew Holt
21 likes to talk about, you know, there are no
22 platforms, there's only data and apps. But, you
23 know, I think it's an important trend for how we
24 think about privacy and how we think about the PHR
industry.

The second is expanding the definition of health information. And I think the point was made earlier that health is not what happens when you go to visit your doctor, health happens 24 hours a day, 365 days a year, it is based on the behavioral decisions you make every day, and it's based on the circumstances in which you live, and it's based on whether you have access to fresh foods, it's based on whether you can walk to a playground, there's all sorts of things like that.

And if you think about health data, health data are things like how well did you sleep last night, what did you eat yesterday, did you get to go for a walk, and again, it's also about your circumstances, whether it's environmental exposures, where you go all day, and what is located near where you go all day.

And this is a major focus right now of Project HealthDesign, is that we're focusing on what we call observations of daily living or ODLs, meaning it's data about your diet, your exercise,
your pain, the mood, the meds you actually took as opposed to the meds that have been prescribed to you.

So now the third thing is sharing, and I think it is so important that whenever we have a discussion about privacy, we think about the importance of sharing, because as important as it is for people to be able to keep some of their data about their health and many other things in their life private, there is a fundamental desire and need to share that information with some people, and we see people doing this all the time.

And so I hope as we talk about privacy today, we think about how do you design systems and design policies that don't optimize first for privacy and then think about how do we share data or how do we let people share data, but really think about those in conjunction. And I'll stop there and hope we come back to some of these.

MR. YU: Thank you, Steve. Darcy, I'd like to turn it to you.

MS. GRUTTADARO: Thank you, and thank
you for inviting me to participate. So we are
sort of in the related technologies area, we're
not really working in personal health records,
although it depends on how we ultimately define
them at some point in time. NAMI is a very large
family and consumer advocacy organization. We
have 1,100 state and affiliate chapters across the
country. And we came to develop StrengthOfUs.org
out of sort of necessity in recognizing that
people in this transition age group of 18 to 25
were not able to connect very well particularly
when they had a mental illness and substance use
disorder, so -- and that we knew they were using
technology to gather information, to connect with
each other, and we wanted to create something that
would be uniquely theirs.

So we developed this online social
networking website. We didn't have privacy and
security in mind at all, that was not part of our
goal. I'm sure all the lawyers in the room are
horrified to know that, but that was not our
primary focus.
And we, in fact, weren't thinking about things like personal health records and sharing of that kind of information, we were more really focused on combating social isolation. What we found, though, is that people, in fact, share a huge -- first of all, the site has been an overwhelming success. We launched it in March, we pilot-tested it for a month, we have 1,300 active users now, which, given that we really went live in late April, we think is pretty impressive. This is a fairly -- it's a sliver of the population, obviously, in this age group.

But what we have found is that people are, in fact, connecting online, they're sharing a lot of information about their health, they share the medications they're on, they share the treatment they're in, they share information about how to address lifestyle issues that significantly impact their health, they provide mutual support about treatment adherence. There's a lot of really good information, support and sharing that is going on on the site.
So I would say that this kind of a social networking approach, and I think it was alluded to earlier on the panel, that we can really incentivize and motivate people, particularly through peer support, when they have similar health conditions, by creating social networking opportunities.

We actually modeled our site after Facebook. We have blogging, we have something that's equivalent to Twitter, it's called The Wire, where you can put in little clips about what's happening that day in your life. We have guest bloggers and experts coming on talking about how to manage schizophrenia, how to manage bipolar disorder, so we're pushing out information because we want to be seen as a reliable source of information around difficult-to-treat conditions.

And the value in this really is that we can get people very engaged and involved and get peer perspectives on what really works and how to live a fairly stable life even with these serious conditions.
So I guess I would say we were a bit naïve on the privacy and security side, and, in fact, we think our data is pretty secure. But I'm probably very naïve, I'm not an IT expert, and people probably could fairly easily hack in or register and come online and begin to use the information that we are collecting.

So there are a lot of -- and particularly with mental health, this was alluded to earlier. Unfortunately there remains a lot of stigma, a lot of myths, and a lot of misunderstandings around having a diagnosis and what that means in the way that you live your life and in your capability and in your employability and in a number of other factors. So I guess I would say I look forward to having a conversation around the value of social networking. As we all know, Facebook is absolutely just enormous and very powerful and important to a lot of people's lives for connection, but also how we can manage the sort of creating innovative approaches like we think we've done while still protecting people's
privacy and keeping data and information secure. So I look forward to having that conversation and I'm happy to be part of this discussion.

MR. YU: Thank you, Darcy. Moving on to John. John, as the only member of the panel who is not directly tied to a I guess consumer health data organization or a PHR, please let us know what your thoughts are.

MR. MOORE: Okay. Yeah, I was an industry analyst in the manufacturing sector for a number of years, and frankly, it got boring, so I was looking for a new adventure and started looking at different verticals and stumbled into health care and started pealing the onion and went, oh my God, what a mess, this is perfect for an analyst.

And then when I started looking deeper and looking at the macro trends in the market, realizing that, you know, increasingly there's going to be a lot more consumer involvement. They're not going to be able to sit back and let their employer just take care of things for them,
that they are going to, you know, as we see more
and more consumer directed health plans with
higher deductibles, what have you, a consumer's
role in managing their health is going to
increase, so that's clear.

So that led to our first study where we
looked at the PHR market and published a report on
that market back in May of 2008. Since that time,
as I looked at this market and looked at how it's
developed and tracked some of the successes, as
well as some of the failures in the market, a
couple of things have become quite clear to me in
the research that I've done.

The first thing is that, you know, I
believe language is a very important thing. And I
think that in having the terms EHR and PHR, we
are, indeed, creating artificial barriers, and
that there is actually only one record, and I
don't know if we call it a unified health record
or a collaborative health record, but there really
should be only one record that is used by the
whole care team and all stakeholders therein.
And I think until we get to that point, we're still going to struggle with these definitions, with these privacy issues, these policy questions. So I think that's one of the things that I see right now. Secondly, as I think, you know, both Dossia and HealthVault talked about a little bit, it's not some, you know, people aren't really interested in a PHR as what has been commonly defined, which is basically a digital file cabinet for their records. People could care less about that, that's why we have not seen very high adoption.

But if you look at where we have seen high adoption rates, there's a couple of things that occur, either the patient/consumer can do something with the data, you know, it's actually actionable, that they can actually make sort of decision based on the information in that record and that that decision perpetuates into some action by another individual, i.e., their doctor, a nurse, what have you, but that's what's important, you know, is it actionable within the
context, and that's why I'd like to just kind of get rid of the PHR term all together, you can call them platforms, I don't care, the unified health record, collaborative health record.

One of the things before coming to this, I actually looked at the table of contents in all the PHR vendors that I profiled in that report back in 2008, and just one after another we click, yeah, they're no longer in the market, no, they're no longer in, they're out, they're out, they're out, you know, and we interviewed, you know, we profiled some 20 vendors, and most of them are gone. It's just -- it's a very, very hard market to actually make work and make money at.

But another thing I've seen is also recently I had the pleasure of sitting down with Gail, who worked with a PHR company. A couple years ago they brought in this PHR to look at how could this be used in the context of delivering better care for diabetes patients and helping diabetes patients take on more ownership to manage their diabetes.
And I'm not going to steal her thunder,
I'll let her talk about it, but an incredibly
intriguing story, and as I wrote on a quick tweet
when I posted this piece that I wrote on it,
basically this analyst got schooled, and it
really, you know, broke down a lot of assumptions
that I had and myths that I had created in my own
mind as to how people may use these things.

And I think that's why we really have to
keep a very open mind as to, you know, as we
proceed forward, you know, certainly privacy and
security are important, but I think it's also
very, very dangerous if we look at this that's
going to be in the consumer's hands and treat it
the same way we treat a physician with HIPAA
inside the context of a health care organization
or institution and how they manage the data. And
I think we can really make it too onerous for
patients and consumers if we're not careful.

MR. YU: Thank you, John. Quite an
introduction for Gail.

DR. NUNLEE-BLAND: Thank you.
MR. MOORE: Well deserved.

DR. NUNLEE-BLAND: I became involved in the PHR about two and a half years ago. I had received a grant from the District of Columbia, Washington, D.C., to explore novel technologies to improve outcomes of diabetes care, particularly in minority communities.

Just to give you a little background, Washington, D.C. has some of the highest rates of diabetes, and the morbidity and mortality in some communities where there's a large percentage of African Americans, their rates are pretty high and the mortality and morbidity is pretty high.

So I explored the personal health record because the care is somewhat fragmented. They move from plan to plan, and particularly with Medicaid population, doctor to doctor, and they never really seem to have a health care with them. And the doctor's office, it's very difficult for them to get their records and so forth. So NoMoreClipboards, I worked with them to integrate -- we were already using electronic medical
record, CliniPro, which is a disease management software geared for diabetes, and we integrated it with NoMoreClipboards. And actually the data that flows over from our EHR to the personal health record is basic demographics, basic insurance information, the patient's problem list, their medications, their allergies, and also labs that we deemed important in terms of their diabetes management, they can actually import their labs.

Also, patients have the ability to track their blood glucoses, they can enter their blood glucoses, they can enter their blood pressure, and so they could really be involved with their care.

Before I even started with this, the question was asked, well, you know, our population, 90 percent of our patients that we see are African Americans, and the majority of them are on a Medicaid medical assistance plan. Do your patients have computers, how are they going to use this, and this is a web-based platform.

So I surveyed and I found out that 70 percent of our patients actually have computers
and actually have access to the web, so this was
not a barrier for them. And just recently I
looked at our data, and now that's up to 85
percent, so more and more are using computers and
the web.

So we've been doing this now for two and
a half years, and we've been monitoring them, and
actually we've seen improvement in outcomes, and
we actually compared it to a group that did not
sign up for the personal health record and to
those that have used the personal health record,
and we saw actually a 0.9 decrease on the
hemoglobin A1C.

Now, that is a blood test that we use to
assess how well someone is doing in terms of their
disease management for their diabetes. And
actually that probably rivals many of the
medications that patients use to manage their
diabetes, and this is just with a personal health
record.

I was really pleased with a lot of the
patients. They would come in and they would ask
me, well, did you see, I entered my data into my personal health record, I got my numbers in there, or I forgot my meter, but it's in my personal health record. And also, they told me that when they travel, if they've gone to other places, if they've gone to an emergency room, they were able to pull up their health record to share with the emergency room physician, so they've really adopted to this particular technology. We also surveyed them because security was a concern, you know, are you concerned about whether your data would be accessed by others, and really only 13 percent had any concerns about security, and even those who did have concerns about security, many of them went on to sign up anyway.

So really only 5 percent of the patients that we surveyed refused to sign up because they were concerned about security, so that was not a major concern to them. They were more concerned about sharing data, having access to their data, and using it in a meaningful way.

MR. YU: Thank you, Gail. And Doug.
MR. TRAUNER: My name is Doug Trauner. I started TheCarrot.com or Health Analytic Services about three years ago. At the time, we were trying to address health engagement. Everyone on this panel is asking the question, how getting people more engaged with their health, how can that make a difference, does it make a difference, and there seems to be some pretty strong consensus the answer is yes, but then how. So if you looked at the market three years ago, there were a lot of great solutions, point solutions, around different programs that people can use online around weight management or getting exercise. Even today, you can go -- there are social networks around different services and conditions or objectives that people are trying to achieve. And that's great if everyone wants to share everything they want to do, but you've got a lot of people who are dealing with real medical conditions and real issues and how do you bring that together.

So we were addressing the question of,
okay, how do you bring together a whole health approach. We see an individual in health like we're talking on this panel, and it's not just if you're dealing with hypertension, yeah, blood pressure and cholesterol levels are one part of it, but also exercise and nutrition, stress management, work time management, it starts to, you know, move very quickly into just lifestyle.

And if you think about so much of the medical costs in this country being around lifestyle related questions, then how are you going to bring together the lifestyle choices that people are faced with making every day, as people are already talking about here on this panel, and bring it together to work in a clinical setting and work in a support setting. There are people interested in helping you achieve your health objectives, as well as on a social level. People are interested in demographics, where it varies by age, but increasingly, there's a lot of people that are interested in participating and sharing that information with other people on a broader
level.

So you see some of that dialogue taking place on very insecure, open places today, but giving people the choice of being able to manage that, bring all that together, again, in a secure manner if you want, but at the same time, the ability to share it within your health care, so being able to address the needs of health care, being able to address social networks, and being able to address your support network for your health care coverage.

So we started TheCarrot about three years ago now. We've gotten some great feedback. We've got a strong user base today, about 50,000 users using TheCarrot. We have a number of about 15 different -- 35 different trackers today of what people can do. It's online, TheCarrot is a relatively consumer-friendly brand. We have an online experience, as well as a mobile experience, what we're bringing live now -- so if you've gone to TheCarrot today, you would see it's a private place. What you do there is for you. You can
record anything you want about yourself,
understand and figure out and learn about
different conditions, different objectives. What
we're bringing now is the ability for people to
start to really share that with these different
groups that we're talking about both in public and
private and addressing the challenges of, okay, if
you're working with -- and the real questions
we're faced with are, if I'm working on clinical
level with my physician and sharing some of that
information with them, and I'm also participating
in a fully open challenge around any of my
measures, let's just say my physical activity,
what exercise am I doing, and I'm sharing that
with maybe even the whole world through that, what
challenges or what are the requirements that we
need to be addressing to meet those requirements?

We've been a locked down, private,
secure place where people can interact with that,
I'm really interested in that dialogue today,
around what do we need to do to make that work.
It's not clear.
Our lawyers, if you ask them to review it, the answer is universally, well, you know, I can't figure this out very clearly, so no, but I don't think that's the right answer. I think when you're looking at addressing health care, and the value of these three areas: clinical, social, and then your health support network, whether it be a nutritionist, physical therapist, people outside of the pure clinical setting, bringing those three pieces together we see as fundamental and I am very excited about participating on this panel.

MR. YU: Very good, Doug, and I hope to address some of those topics during this session. It's a very exciting time for innovators in the space, especially with a great deal of volatility. Demographic trends are changing, and technology development continues at a rate that's unabated.

Let me throw out a question first to the folks who are championing organizations directly working with consumers and patients. What are the evolving trends that you see in terms of consumer or user demand?
Darcy, you mentioned social media; Gail, you mentioned that the technology literacy of your population is ever increasing. With respect to health data, with respect to PHRs, are there any trends or issues that you see? Darcy, let me throw it out to you. And hopefully both Steve and John can comment on how the innovators are responding from a commercial organizational perspective.

MS. GRUTTADARO: Yeah, I mean, I would say I think there's a real interest in managing health conditions, and I think that presents a tremendous opportunity.

MR. YU: And this is at an increasing rate or --

MS. GRUTTADARO: At an increasing rate. I think people are recognizing there's a lot that we're hearing about in just the sort of mainstream media about managing your health condition. And I think also there's, in the mental health world, which is the world I operate in, there's a lot more recognition that people can do more, so
there's sort of incentives to manage your condition better.

And I think there's also a real interest in connecting with others who have the same lived experience, because I think there's sort of a -- there's a kindred spirit aspect to this, like you're in the same boat I am, you understand my health condition as well as I do, so that connection among people with the same condition I think is very important, because there's sort of this perception that people understand better when they're in the same boat as others.

So I think -- and the other thing is, I think just reaching out for support when people are at different stages of resiliency raising and recovery, so recognizing that other people that may have a health condition may be farther down the road than you are and may have a lot to share in how they got to a point of being deeper in their recovery phase.

So I think all of this lends itself to creating connections. And I like the way actually
Doug presented this in sort of a three part way. You know, there's the clinical, there's -- I don't know if I'm saying this right, but the lifestyle and the social, the sort of -- you have to -- if we're going to really do well in the health care world in this country and control costs, I mean we have to really be thinking about how do we incentivize people in all of those areas, and social networking is one way to do that, and I think we're seeing that more and more, and we're seeing that in the work that we're doing.

MR. YU: Very good. Gail, would you like to respond to some of that social aspect?

DR. NUNLEE-BLAND: Okay. Well, you know, one of the things that we implemented just recently, over the last six months, has actually been cell phones, we've been using the cell phone technology, and we actually are finding that patients are really -- they really like that because they always have their cell phone with them. And so now they're entering their blood glucose and the cell phones integrate with our
personal health record and it is uploaded so that
they don't have to enter dually, and the patient
says I always have my cell phone and I prefer this
as a way of communicating with my doctor.

The other aspect of it, which I think
has been very helpful is that with the cell phone
technology that we've integrated, it gives them
alerts and reminders, have you had your eyes
examined, is it time for the podiatry visit, have
you had your flu shot. And so, again, because the
cell phone is with them at all times, it gives
that that reminder, as well as your appointment
time. And then there's questionnaires that we
sometimes ask them to keep them in tune with their
health.

So using these multiple medias really I
think engages people. And I'm sure the social
media, we haven't quite got into the blogs and the
Facebooks yet, but I think it really does help in
terms of management, that the patient is the one
that is involved with their care, and that they
should be in control of what they're doing, and
the more they can interact with their health care providers and other people around in their social network really is of benefit. Another aspect, too, is they can add other members or other families or other support to their network so that if they need an alert or reminder sent to a family member or a friend, they can elect to do that, as well, and that has been very helpful.

MS. GRUTTADARO: I just want to say one other thing, too, about the sensitivity of information, because when it comes to mental health, and I'm sure this is true for other health conditions, people -- it's not a topic or a subject that people feel necessarily comfortable always approaching a medical professional about, so they're seeking information online, and they can really -- the more we can provide information on sensitive topics that's reliable, whether it's through social networking or -- I think it's -- people increasingly have turned to online resources for sensitive information and for conversing on sensitive topics, and this is
particularly true in mental health and substance use.

MR. YU: Right; Doug, do you see any special populations with emerging needs, or I guess --

MR. TRAUNER: I mean there are the standard breakdowns of disease management and sort of health improvement that we -- when we look at what people have been doing on TheCarrot -- it sort of tends to follow, you know, weight, exercise, nutrition, and then chronic conditions, diabetes, asthma, hypertension tend to be some of the activities that people are trying to participate in, we've definitely seen an uptick in the number of people have been using the service, that are getting engaged and participating in that.

To be fair, our social aspect is what's coming on now, the social's been mostly around what people want to see from the site. It's been very consumer-driven by what kinds of things people want to be able to track, how they want to
be doing that better and we've been responding to
that.

But what we're bringing now is the
ability to share all that information and
addressing that. So we're definitely seeing an up
tick in terms of how people are interested in
participating in what we're doing, as well as
also, we're getting a lot of companies that are
saying we'd like to be able to bring this quickly
to other wellness companies that are saying we'd
like to use what you're doing, but we have some
ideas of how we want to package it up, and we're
working with them, as well.

So I think there's a lot of interest in
companies saying look I don't want to be building
the technology around this, what we want to be
doing is taking and putting programs in place that
can make a difference and helping them to achieve
that, as well.

MR. YU: John, if you could comment.

Are these trends that you're seeing in the wider
spectrum with regards to emerging needs and
innovators that fill them?

MR. MOORE: Well, I think right now what I'm seeing is, in the market, is a couple of things. First off, and I was talking actually to one of the innovators out there in the market this week, and I asked him what is he seeing in the market, and he says, you know, on the provider side they're seeing nothing, the providers are -- and even amongst providers, that even will talk to them, it's still about marketing and consumer retention.

Basically, you know, they put up the PHR or the patient portal, but it's all about retention of the patients so they'll keep coming back to that particular institution for their care, so it's a marketing play.

Where they're seeing some traction is, of all places, in the HIE space. As regional -- in particular, regional exchanges are looking at how do we become sustainable over time, and they're looking at, okay, is there a way that we can start providing, particularly around what this
particular firm calls care units, but looking at specific chronic diseases and creating within the context of a RHIO or an HIE, care plans around that to help people in that community share information amongst each other, as well as promote the care around say diabetes, or maybe in mental health.

You know, right now they're really looking at the typical chronic diseases of diabetes, you know, COPD, things like that, not necessarily mental health, but I think what we're seeing in the market in general as a trend is -- I hate to call it disease management because disease management right now has a bad name out there in the market, so I really don't like going down that path, but it's more personalizing the platform around specific areas of -- to help people actually manage their disease, their care, personally, on a personal level.

And getting to Gail's point, yeah, you asked I think in your previous question what do we see three to five years out, and for me, all I see
is mobile, mobile, mobile, mobile. It's with you wherever you are, and, as I like to say, health is mobile, it does not happen in front of your desk top, it happens wherever you happen to be, and the only thing that can really provide that capability is a SmartPhone or even a feature phone with texting features.

MR. YU: Very good; and Steve.

MR. DOWNS: Yeah, this is an interesting question. I agree with a lot of the same trends. I think one of the most important things to hear is, this is a time of rapid experimentation, and things are evolving, they're not figured out, the industry hasn't sort of jelled, and in some ways I defy you to think about what a personal health record is, and, you know, and really then try to regulate it, you know, and good luck.

And so I think the -- and then just a way to express that, if you think about some elements of personal health data and how you use them, there are input devices or input opportunities, there are storage and maintenance,
and then there's also sort of the display and action triggers kind of thing, and you think about diversity of inputs.

You can gather health data from sensors, you can gather health data from SmartPhones, you can gather health data from somebody sitting down and typing something in, you can gather health data from an office visit. If you think about storage, you've got places like TheCarrot. Think about Nike Plus, Nike Plus has an unbelievable number of users entering data about their exercise every day. Every app on the iPhone store is tracking somehow—all 6000 health apps, you know, they're tracking data about you. HealthVault, Google Health, and then, of course, you know, the Kaiser model, as well, has a lot of your health data.

And actually Twitter, you know, I mean I remember following somebody who was tweeting his weight every day for a while, he stopped after a while, but --

MR. MOORE: Was that a good thing?
MR. DOWNS: That he stopped?

MR. MOORE: Yeah.

MR. DOWNS: No, but -- and, you know, there are actually people that are working on sort of secure ways to use Twitter as a platform for storing your data, and I can talk more about that.

But then also again, think about how you access these data and use them. You know, again, you can log on from a PC or you can be hit by something on your SmartPhone. So again, thinking about the concept of a record, when information is this distributed and takes so many different forms and it is changing every single day I think is a real challenge.

The other thing I wanted to speak to in terms of the trend, you know, and I mentioned this observations of daily living idea earlier, you know, so there's a group that started out in the Bay area called the Quantified Self, and there's a great article in the New York Times magazine from about six months ago by Gary Wolf, who's actually very involved with the movement. And so
Quantified Self is people -- and these are -- it started out very much kind of sort of the Bay area geeks, and I say that in the nicest possible way, because I love them, and these are folks who professionally have learned the value of tracking data and using feedback to make systems better.

And so they say why not apply this to my life, you know, so these are people who track exactly how long it takes to drive to work every day based on the day of the week and the time they leave the house, and then they say, well, what if I left five minutes earlier, and then they say, you know what, I actually got there ten minutes sooner, you know, and so they do this constantly in their life and they're starting to apply it to their health.

And it was great when Gary's article came out because, you know, there are all these things on the Times website, and people are saying these folks are crazy, they're really weird, you know. But what's actually happening is, it's starting to go mainstream. So Quantified Self now
has chapters in 12 cities. And Susannah Fox from the Pew Internet and American Life Project is working on a report, it's not published yet, but she has actually released these data points which say that 15 percent of Internet users are tracking diet, weight, exercise online, so they're putting their own data online, 15 percent of Internet users, and then 17 percent are actually tracking symptoms besides diet, weight and exercise.

So, you know, we have really moved from the alpha geeks to a much sort of an early adopter part of the curve. So I think this is a trend that is -- that we need to be paying attention to.

MR. YU: Thank you, Steve. Steve, originally you brought up a point about the separation of the apps from the data, and we've heard a discussion around new collection modalities for what seems to be an ocean of data that's emerging. I'd like to throw out to the panel, what are the new types of analysis and new applications that are taking place as a result of this data? You know, as the data becomes stored,
especially in an identifiable form, what do we see as future iterations of analysis, applications specifically designed for the end user either in a social sense or in an individual sense? I'm going to throw this out to Doug first since your organization seems to be very nimble in terms of collecting data. Can you speak a little bit to this point?

MR. TRAUNER: Sure. I think there are a couple different ways to look at the analysis, part one, just the ability to look at all the data in a meaningful way, in a simple way, in a non-aggregated way, so just showing a week of your information at various times, how people look at nutrition and what they're doing. You can even do it with pictures, for example, being about to just see that information. So there's just the immediate -- there's a feedback story and people can respond to that.

MR. YU: Longitudinal, right?

MR. TRAUNER: There's a longitude, exactly. And then being able to compare that with
other different measures that you're looking at.
So it could be your mood or your symptoms and are
there relationships between those, and that starts
to get another type of, well, what is going on
with my blood pressure when I'm getting exercise
or not getting exercise, those kinds of questions
that, on an ad hoc basis, people like to look at.
You then start to have another set of
questions that come up, especially when you start
to tie into clinical, they don't want that
information necessarily. Providing, you know,
there are great stories of people using The Daily
Plate, and they show up with the report, which is
15 pages of everything they ate, and they're
sitting down for a 15-minute visit, and it doesn't
facilitate the conversation, it's more, well,
that's interesting, now tell me what's going on.
So the ability to then structure very
consolidated, very meaningful reports that a
physician in a clinical setting would be relevant
in a succinct way, as well as not, quite frankly,
introducing a new type of legal liability.
If you give them all of the information and they then are responsible for going through and figuring out, is there a problem that I need to respond to, and they're not getting paid for that, so addressing that question in a succinct way that makes sense for them, this is their report in a succinct way for diabetes, it doesn't have extraneous information that they didn't want to see, those are kind of three areas that we're addressing right now. Does that kind of --

MR. YU: Yes. Gail, would you just like to speak a little bit about the diabetes related data that I guess you're collecting and the applications that might be generated as a result?

DR. NUNLEE-BLAND: Well, you know, we always like to look at glucose trends, so that when we can see that and see patterns in terms of where their blood sugars are going, we can make adjustments in terms of their medications, so that is very helpful to us, also the trends in terms of some of the other labs that we look at in terms of how well the patient is being managed in a useful
And I agree with you, we really don't want stacks of papers, but we want something that is sort of consolidated because we really don't have a lot of time. And so when we can get data that is consolidated or at least graphically displayed to us or averaged out, that is very helpful to us in a clinical setting.

MR. YU: And is this something that the users are requesting, as well, or are responding to?

DR. NUNLEE-BLAND: The users, really all they -- if they enter their blood sugar, they're just entering their blood sugar. But I want an application that would average it out to me, let me see the trends. They're not concerned about, you know, whether it was an average or whether -- all they want to do is put their data in and hopefully something goes in a black box and it does the work for them. So users pretty much want things simple, and that's what I found in terms of our set-up, that really users don't have to put a
lot of data in, because there's a lot of transferred data back and forth between our systems, so they like that part of it, and then it will graph it out for us and we can begin to look at averages and so forth.

MR. YU: I see, so from a clinician perspective, okay, very good. So, Darcy, would you like to respond from a --

MS. GRUTTADARO: Yeah, you know, it's funny, when you first asked the question, I was going to say, well, we don't really -- we're not really looking at the data in that way because we're really a social networking site, but then I remembered that, yes, we are actually looking at what people are blogging about and tweeting about, and we're looking at what their questions are, and we're sort of looking at it in an unscientific way to say what are people saying about their treating providers, what can we communicate back through our advocacy work and our policy work to provider organizations that can have an influence on how services are delivered. We're thinking about what
kinds of information are people seeking that may
not be available in their communities and from
their practitioners, and how can we supplement
what they have so that they can better understand
what the research is showing, because,
unfortunately, mental health, a lot of what's
delivered is not evidence-based and is not leading
to positive outcomes and we have a long way to go,
so we are educating consumers about what kinds of
services they should be getting.

If you want major depression, are you
getting cognitive behavioral therapy? If you're
not because there's not a provider in your
community that's been trained in that, we have
work to do to advocate, to ensure that providers
are trained in the most effective intervention.

So, in a sense, you know, my initial gut
reaction was, we're not really looking at the
data, but we are, and we're using it to say there
are some overriding policy issues here and how we
can better address the needs of this demographic
so that we can produce better outcomes.
We can bring down our overall health care costs, we can keep people working, we can keep them living in the community, we can do things that will make communities healthier and will lead to lowering an overall health costs. So we are looking at the data, and I think it's -- there are a lot of important social change that can happen from learning about what's going on in these social networking sites.

MR. YU: Steve, any implications in terms of application development?

MR. DOWNS: Well, I mean so one of the things that we are focusing in on Project HealthDesign is, how do you tie back to the clinical care team, and I think a lot of what's been said, whether it's by Gail or Doug, you know, that you have to figure out how do you fit both into the time that a clinician has and also their work flow.

And so each of the teams that we're supporting are looking at what kind of data are we gathering in terms of people's day-to-day lives
and then how do you both analyze it for sort of clinical signals, I guess I would say, separating the signal from the noise, and then how do you display it in a way that's useful, and then again, how do you fit it into the work flow. And I won't say that we have answers yet on those, they're sort of -- the projects are kind of in flight. But I also want to bring back an analogy, and I owe this, again, to Susannah Fox, which was, she pointed out that about 15 -- 16 years ago now, people started walking into their doctor's offices with reams of paper from Internet searches they had done about their conditions, and some of the doctors sort of said, you know, get away, you know, this is not the proper role of a patient and all that stuff on the Internet is wrong anyway, and some said, this is really neat that you've actually taken this time to do that, and, you know, it's probably not the best thing just to bring me a stack of 30 pages of this, but let's start to have a conversation about how we can have a dialogue that's informed by your
research.

And she was saying we were going to start -- we are starting to see and we're going to start to see more of the patient who brings in, you know, the 30 pages of sleep and exercise data. And again, some docs will say don't you ever do that again, and others will say, okay, that's not a helpful format, but the idea is right. And I think it's interesting to think that this may actually be a legitimate analogy. I mean, I think that it's an open question.

MR. YU: Very good. And, John, do you want to talk a little bit about the long tale of applications?

MR. MOORE: Well, yeah, I think one thing that has not been touched upon, because at least based on what I've heard so far has been patient-clinician, clinician-patient interchange. We haven't talked about patient-to-patient interchange.

And what they're doing in terms of sharing information, you know, we mentioned --
Darcy mentioned something about social networking, and, you know, they have a blog and some tweet type capabilities within their site that they developed, and there's a fairly well known site that we talked about quite a bit, PatientsLikeMe, which has become somewhat of a legend in the sense that people share incredible amounts of information, knowing that that information will be, you know, what pays the bills is the pharmaceutical companies, but people are still willing to share information on this because it helps them help each other, and they have just intermediated the clinician from the equation.

And there's a number of different stories that, you know, both Jamie and Ben that started this site can tell you, but just a quick one, for example, was, there was a clinical trial in Italy saying that lithium helped mitigate ALS, and addressed some of the symptoms of ALS, which is basically a death sentence. So a bunch of, you know, PatientsLikeMe started around ALS because their brother died of ALS. Anyway, 300 people
started taking lithium. They found out very quickly that it did not work. How long would it have taken us here in the United States to set up a clinical trial with the IRB in a clinical institution to actually get to that result? It would have been years, they found out in six months.

So I think we really have to start thinking a little bit more broadly instead of just physician-patient, patient-physician, we really need to start thinking of health care, how do we as a community address health care and help each other.

MR. YU: This level of intermediation, do you think it's an isolated case or do you think --

MR. MOORE: Absolutely not, absolutely not. If you -- and I'm talking about PatientsLikeMe, but you can go to Navigating Cancer, which has all sorts of forums on various cancers that people go there and share their experiences, share, you know, what kind of
medications they're on, what kind of side effects
they're experiencing, how to address those side
effects, there's no physicians there. These are
patients helping patients.

MS. GRUTTADARO: Yeah, that's all
StrengthOfUs.org is about, that we are totally a
peer-to-peer, it's all people living with, so
that's what they are. We don't interject, it's
their community, they're talking to each other,
that's all what we're about, so I just wanted to
clarify that, yeah.

MR. MOORE: Okay.

MS. GRUTTADARO: And it works. I mean
people are really -- people really share a lot of
information around treatment medication, treatment
approaches, and how to stay healthy and all of
that, so I just wanted to clarify that because I
might not have explained that.

MR. MOORE: Yeah, and I think from a
policy point of view, when you start thinking
about privacy and security, you really have to be
very, very careful, because people do want to
share information to help each other.

MR. DOWNS: And I think that part of what they get out of the sharing is, they get personal value, as well. So it's not just sort of communitarian and altruistic, you know, I want to give my data to the greater good. Paul Wicks is the Research Director at PatientsLikeMe, he gave a talk recently in which he said in effect, and I'm paraphrasing, we are religious about providing feedback to every piece of data that someone submits. So even if we do a questionnaire that says do you like the new design of these pages, and you say yes, they immediately give you something back that says, well, you're part of the 29 percent that likes it, because 71 percent don't.

So everything you do, where you say this is -- I am now taking 100 milligrams of this thing, they will say, that's funny because 75 percent of people are taking 200 milligrams and you're taking 100. And he's saying you're immediately giving value, you're essentially, you
1 know, again, this is not his word, but you're
2 essentially training users that when they do
3 something by sharing information, they're going to
4 get something back that really helps them.
5
6 MR. YU: Very good. I want to touch on
7 the security and privacy aspects of the discussion
8 so far, but before I do so, Gail, you know, would
9 you like to share some thoughts as a clinician,
10 how do you respond to, you know, the patients I
11 guess acting at this level with response -- with
12 regards to their own data?
13
14 DR. NUNLEE-BLAND: You know, it's just
15 interesting, and I guess, you know, I'm surprised
16 that there's a lot of concern about the security,
17 because, you know, when we surveyed our patients,
18 they were not that concerned about security, so
19 from a patient's perspective, they didn't see --
20 they saw it as a benefit that I have my
21 information, I have my problem list, I have my
22 medication list, I have labs, you know, because
23 patients call, it's very difficult sometimes for
24 them to get their results, and so that wasn't a
major concern to them.

Now, I guess who will eventually get the data maybe that is, and I think concerns about whether my insurance company will get it and do something with it or my employer, I think that may be where the concerns are.

But I think the way we have it set up where it is just between the provider and the patient, and the patient has that data and takes it to another provider, they feel as though they have more ownership rather than a covered entity providing it or an employer providing it and what are they going to do with it. So I just found that less than five percent really just refused to sign up for it because they were concerned about security.

And from a clinician's point of view, if I can have accurate data from a patient that I know that is provided by a provider, that I know that the medication list is correct, the problem list is correct, the labs have been imported, you know, correctly, that facilitates my care. If
they happen to be seen at another facility, they come to my facility, I can look at that and feel fairly confident that I will treat this patient appropriately versus not having any information at all.

MR. YU: Very good. Darcy, are the views with regards to security and privacy shared by your user, your audiences?

MS. GRUTTADARO: Yeah, well, I did read a little bit of the FTC report, which was 122 pages, so I didn't read the whole thing, but -- and I was very impressed with the discussion around the fact that I think a lot of consumers really don't appreciate when they share data and information, what that really means.

So I think in terms of a regulatory role when it comes to privacy and security. And I think the report really alluded to this very nicely, we need to really make sure that people understand what the implications are when they share data, and we need to do that in an easy to understand manner. And it's funny, this week I
did a webinar on mental health screening, and as soon as I disconnected from the webinar, I got an email in my email box from a vendor that was selling mental health screening tools, and I just thought, oh my gosh, this is wild. I mean it just occurred to me that I am so naive in my professional role even of, you know, how information is being used in an aggressive way.

So I think one of the areas, and particularly with mental health, although I hope we can some day normalize mental health as any other health condition, we're not there yet, but I hope we can, and so it does get included on EMRs, and people aren't afraid to have it on their personal health records, but we are definitely not there yet.

So I think one of the things in general is making sure that people understand how their information can be used and the vulnerabilities. And I think we could go a long way if we did that, even the developers. And we have to make it easy, and we have to make it easy for the people that
are developing these innovative approaches to connecting people like we are.

We create a peer-to-peer site, we don't fully appreciate, and we have lawyers that look at it in the end, but I don't think that the typical person who's using these products and developing them has a real grasp. And I just think we've way over complicated the whole data and privacy world, so I think we have to figure out a way to simplify it more so there's an appreciation.

MR. YU: There's an appreciation, but there's room for education.

MR. GRUTTADARO: But there's room for innovation. And I realize that's a -- there's a real tension there, because I think rapid innovation, as Steve was alluding to the fact that this is, you know, an exciting time, can lend itself to exploitation.

MR. YU: Doug, would you care to chime in on this?

MR. TRAUNER: So I mean there's clear disclosure of information. I think the Microsoft
discussion, the previous panel had very clear and
obviously were addressing them in a very similar
way. As people are sharing information, there's
transparency. But I think the discussion here is,
are people understanding it? Is it easy to use?
Is it clear? If information is being sent
somewhere when you enter it, is it listed in one
simple place that you can easily access it or do
you have to navigate through four or five
different places to actually understand that? And
I think, you know, the discussion here is about
privacy, but it keeps coming back to what was on
the previous panel on trust. And I think also the
point of if you ask people how big of an issue
privacy is, you'll get sort of two ends of the
spectrum: One, it's incredibly important to me,
or it's not important but it becomes important to
those people when they realize something, like you
were telling the story of now you're going on the
web and you're seeing the ads run, you kind of
wonder how did they figure that out.

I mean, everywhere I go on the web, I
see a PracticeFusion ad, I don't know how they
know that I would be even remotely interested.
But it's the same question of, as people are using
these services, the ads are remarkably
coincidental, then there's concern, well, how did
they know that, and if they're seeing that when
they're now on other websites, I think that's
where people are starting -- I think the FTC is
now actually addressing that discussion, and I
think that's incredibly important, and it sort of
says if I'm using this site, how is it being used
as I'm no longer on that site.

And, you know, there are people --
there's a lot of -- I think the other part of the
question is the monetization of these kinds of
services. The reason the ads are being sold, the
reason that people are selling this data is, there
really isn't a monetary -- there are real
questions about how to monetize these kinds of
services. Physicians are not reimbursed, a large
percentage of them, based on certain, you know,
doing electronic visits, so I think there's a
reimbursement set of questions.

So if you look at the success of the vendors in this space, a lot of it does come out to some of the reimbursement models for electronic activities, and that those they are not in place. So I think there is a series of broader questions, as well. But certainly the privacy, obviously we're addressing it in a technical way, and, you know, I have a personal letter up there about how -- what does it mean in a summary way about look we're not sharing it, we don't sell it, we're not -- this is about you and your privacy.

So trust, but I think there's a broader set of questions about how to facilitate these interactions which could significantly reduce total health care costs, but there needs to be some means of a financial model to make it work, and today that is not really in place.

MR. YU: Do you agree with Darcy's point that users may not be fully cognizant of the implications of the --

MR. TRAUNER: I think most people when
they accept applications and then look at the
terms of use and then start scrolling through it,
no. I mean, there are -- I mean, a lawyer
reviewing it, it's still going to come back with
ambiguity. I think they tend to be very long and
confusing, they have to be because they're legal
documents. But how to summarize it, even getting
a sign-off on a summary statement of what that is,
that can be difficult.

So, no, I don't think it's -- I don't
think there's a simple way to be addressing the
legal requirements and to make it intuitive. You
have to do it, you disclose it, you report it,
and, you know, the fine print allows a lot of
latitude, and I think it comes down to the trust
of the organization that you're working with to
know are they actually in alignment with what I
want to achieve.

MR. YU: Very good. Steve.

MR. DOWNS: Yeah, I'm certainly not the
first person who said that, but I think a lot of
the times it simply boils down to control, to be
able to control who sees your data and who
doesn't. And just two quick anecdotes on this;
one is, we had a grant in Project HealthDesign to
the -- it started with the Art Center College of
Design, and they were working with teen
population, and everybody said, oh, it's those
crazy teenagers, they just put everything up
publicly, they don't care at all about this, and
really what they got from their research was, no,
that's not at all true. I may share my behavior,
my mood, my health conditions with the 80 people
that I choose to share them with, but you better
not let my mom see any of this, you know. So it
is actually a very fine-tuned control, it's just
their parameters may be a little different than
some of ours.

The second anecdote is, I was actually
on my way to a conference on health information
privacy a couple of years ago, and I was talking
with the cab driver, he was asking me where I was
headed, and he said, oh, wow, health information
privacy, that's a big deal, that's really serious,
you know, I mean, like, god, you know, I wouldn't want anybody to know that I'm on, and then proceeded to list three medications that he was taking.

And to be fair, this was not my first cab ride with him, we had had a couple of conversations before, but again, the point is, he chose to share it with me, and he was very worried about other people having that.

And then last thing I would say, also speaking with control, is, I'm very interested in the notion that people should be able to sell their health data. If you think about it, we sell our personal information all the time. Any of us that has those supermarket cards that give us discounts, tell them everything that we buy, you know, we're making a deal, whether we know it or not, we're saying, you know, this is worth a certain amount.

I'm quite happy to sell my privacy about what I buy as long as I get, you know, $7 off every time they go shopping in your supermarket.
So, you know, people's health data have value, clearly, and I think people should be able to think about and have platforms where they can negotiate the sale.

MR. YU: Steve, as a funder of innovators and future development, could you speak a little bit about, I guess, what are the concerns from the development community with regards to security and privacy and how they're, I guess, trying to operate an environment, develop new operational models without a great deal of clarity or assuredness of what will ultimately be born out?

MR. DOWNS: Yeah, you know, I'm not sure how well I can speak to that, except -- as I think you almost put the answer in the question, and we heard about it a little bit this morning, and we certainly heard it from Doug, and I think he's a really good person to talk about it, which is, it's about the clarity, you know, it's about not quite understanding the environment, the legal environment, about what you're developing to. You
know, I mean, one of the great things about
developers is that they need very clear
requirements and then they force you to know what
you want so that they can build it to that
specification, and when things are unclear, it can
be frustrating. And, Doug, I don't know if you
want to jump in on this.

MR. TRAUNER: On the clarity of
development or --

MR. DOWNS: The clarity of rules around
privacy and security in terms of being able to
offer a service and knowing what's okay.

MR. TRAUNER: Sure. Well we address it
from the standpoint of the ability to create
relationships, would it make a very clear what a
relationship is and what information will be
shared in that relationship and the other part is
that both parties are accepting the terms of that
relationship and either party can terminate it. I
think that's standard technical requirements for
doing that, but I think your point is on a broader
one of how to make that intuitive and obvious to a
user when they're going to decide and to make that
too much seem actually make sense. I don't think
most people are used to signing up for services
and accepting terms of use on a broad level, but
you seem like you have another question.

MR. DOWNS: Yeah, I was thinking more in
terms of the experience, when you seek the
lawyer's review of what you're trying to do and
they say --

MR. TRAUNER: Oh, there's --
MR. DOWNS: You know -- we're not really
sure, so why don't you --

MR. TRAUNER: Yeah, I mean today with
most of the discussions, and we want to be doing,
you know, X-service, I can pretty much guarantee
the review that we got, after a very expensive
review, is, we don't quite understand it, the laws
are ambiguous, and we think you can do it, but
actually it's not an explicit, yes, you can do it.

And so I mean it's traditionally couched
from a -- so I think getting points of
clarification about what it means to be
communicating with -- when you're receiving physician-messaging over a system, what does that require.

So now you have, you know, a partner agreement with, on a clinical side, and you have to have terms that support that, and at the same time supporting other types of communication that may not be meeting those requirements, it becomes -- it's not entirely obvious how to do it, and those are the questions that, you know, we're really trying to figure out right now. If anyone wants to give us clear guidance on it, we'd love to have it.

MR. YU: John, you wanted to chime in on this, on the innovation development?

MR. MOORE: Yeah, it's been mentioned many, many times already, so I'll just restate it. It's really with regards to trust, trust, trust, trust. I'm a Mac fan. I get my little software updates automatically. I go to -- say yes, I want to update, and then it has some privacy, you know, some sort of agreement, do you agree to this user
agreement, and I look at it, and it says it's 56
pages long, I agree, okay, done.

I trust Apple to do the right thing and
install the Apple fix, I don't worry about that.
Sure, I've got 56 pages of text I could go review,
do you think anyone is reviewing that, anyone?
No, it's done by lawyers for lawyers, and I don't
even think lawyers who are using Macs read it.

So that being said, I think we really
have to put it in context of people trusting who
they're working with and who is holding that data.

My hat's off really to I think Microsoft, for
example, has done a very good job in creating a
privacy agreement that is very simple and straight
forward to read, and when they launched -- shortly
after launching HealthVault, I tried it, and I
said, well, what about all your third party, you
know, vendors on the ecosystem, what about them,
and they actually said, yeah, good point, so they
got all their third party vendors to sign that
same agreement, that when they come onto the
ecosystem of HealthVault, they agree to the same
terms and conditions that HealthVault already
agrees to with the person that's using that site,
and it's very simple language.

Of course, they've got more language you
can read if you wish, but the basics are right
there, we will not use your data for anything, we
will not sell your data, it's very simple and
straight forward, and I think that gets to -- and
then that gets to the whole issue of trust, and
whether or not people trust Microsoft is a whole
another ball of wax, but personally, myself, I
trust Microsoft with my health data more than I
trust my hospital, simply because they have a
very, very big vested interest in securing that
data, because if anything happened and they had a
breach, can you imagine the PR nightmare Microsoft
would have on its hands? It would basically just
blow up in their face. My hospital, if they had a
breach, gee, well, sorry, guy, we'll try not to
make that happen again, but, yeah, your records
got breached, your social security number is out
there somewhere, who knows where, as long as, you
know, you're a Blue Cross/Blue Shield member and
everything else, and we'll try to make sure no one
hacks you, that's it.

So I think it really does come down to
educating the public as to what are the
vulnerabilities, and then letting them make the
decision as to who they trust.

MR. YU: Very good. Well, we're about
to reach the end of our time. What I'd like to do
is I guess let each of the panelists respond in a,
you know, two minute response of any closing
thoughts that they have as a result of the very
fruitful discussion that we've had today, you
know, reflecting on the pace of development, the
pace of consumer demand, but also the
privacy/security concerns, liability concerns, and
I guess I'll throw it out. Does anyone want to
start off with that? Otherwise, I'm calling
someone.

MS. GRUTTADARO: I'm happy to start. I
just want to -- I've learned a lot from the
StrengthofUs.org project we've done, and I think
social -- I'm a big fan -- I'm not on Facebook, and I don't want to be on Facebook, so all those people who are chasing me out there who keep saying you've got friends, I'm not responding. But I do want to say that I am now a big fan, and I think for people with chronic health conditions who want to connect with others who have similar experiences and challenges in life, it is going to be very explosive.

And we're just one little piece, but this is I think something that we are going to see really explode as people are looking to connect with others with similar experiences.

So I just -- I quickly made a note of some of the value and benefits of social networking to people with chronic health conditions. There's mutual support, there's access to reliable information resources, there's connections with peers, there's idea sharing on medication, treatment, therapy, and there's increased resiliency and opportunity for recovery, and there's combating social isolation that often
comes with chronic health conditions, which I put
last, but was really the reason we developed the
site, because we've seen all of those other things
really evolving.

So I guess I would say to ONC and the
FTC, you have a job in front of you, because on
the one hand, I think it's important to encourage
the sharing of information and innovative
technologies that can really connect people with
chronic health conditions in these important ways,
and help to lower our health care costs, and help
to result in improved outcomes for people with
chronic health conditions, but we really have to
be careful about the inherent risks of data
information sharing that can come with people that
have chronic health conditions.

MR. YU: Very good. Anyone else?

MR. DOWNS: Sure, I can jump in. Just a
couple of things that perhaps we haven't touched
on as much that I thought it would be useful to
get out there. One is just really to talk about
sensors and just how that's emerging and the kind
of data that you can get off of it.

So I think in the marketplace they're starting to do things like Fitbit and Zeo that can track, you know, Zeo tracking your sleep patterns and Fitbit activity and other things like that. A couple of Project HealthDesign projects, Carnegie Mellon University is tracking sort of literally the activities of older people as they go about their lives within their apartments. And so, you know, looking for things like cognitive decline, are they getting confused when they're making their morning coffee, are they spending the whole day in bed, you know, so stuff that they can do completely passively without anybody noticing, including, you know, are you taking your meds.

We actually, believe it or not, and I'm not making this up, one of our grantees is working with premature infants who return home from the hospital, and you really do have to monitor quite a bit. They've actually figured out how to sensor baby poop and look for, you know, nutritional content on it, you've got to love it.
But -- so my point is just that this is really starting to happen in ways. And in a lot of cases it's one layer of the sensing and then a whole sort of analysis layer, which is actually converting that basic raw data into interesting and useful health information.

And that bridges to another point, which is that what is health information is very hard to define right now. So Sandy Pentland at the MIT Media Lab has done a study of -- he looked at German geolocation data from cell phones and was actually able to predict diabetes in something like 50 percent of users based on their geolocation data. So where they're going all day is actually a predictor. But if you think about it, I mean, you know, just a really simple example, you go to, you know, you go back and forth to an HIV clinic, and that's on your cell phone, you know, so that's, in effect, disclosing your status there. So I think anything is potentially health information, which I think makes -- you have to think about, you know, if
you're trying to create policy around health information, it's really about information more generally.

MR. YU: Very good. Gail, a brief response?

DR. NUNLEE-BLAND: I just wanted to, as we're developing these medias, if we can identify what is patient-entered versus health care provider-entered so that we know where the data came from, I think that would be very helpful.

MR. TRAUNER: Following up on Steve's comment, I think there's one part of the conversation that's -- maybe it's out of scope right now, but if your sensor information were to flow to a physician, there's another regulatory agency, the FDA, who's also stepping into that process and requiring FDA approvals if it's going to a mobile phone. So I think there's another level to if we're trying to facilitate this kind of communication and we see value in it, it starts to become another layer of regulatory questions, or are there ways to have things expedited or
reviewed, what are some ways to make that work easily? I think there's some incredible opportunities. I think there's some incredible innovation going on. And what people are bringing from a clinical perspective or a research perspective and bringing that to market quickly, there's some really interesting ideas. So helping to facilitate that, it would be great.

MR. YU: Thank you, Doug. In closing, John?

MR. MOORE: In closing, okay, thanks, Wil. Well, I guess in closing, I think what I see as most important is that we really have to continue to educate the public about the use of the -- the appropriate use and the safe use of this information and the sharing of that information.

And when I say the public, I'm not meaning just the patient consumer, I'm also saying the physician, because I still think we have a really big issue with physicians willing to use and trust this information when someone shows up
at an appointment.

And to Gail's point, I think it's very important if, you know, talking policy, that, you know, we need to create these systems if we're going to be sharing them with physicians that have some way of preserving the true medical document, that if a patient wants to annotate that, then that's fine, but they can't change the core data elements within that medical piece of information, like a lab result. And I don't think we have very clear policy and rules around that, and I think that's something that does need to be addressed.

MR. YU: Very good; well, I'd like to thank each of the panelists at this time, and a round of applause for our guests. [Applause].

MS. PRITTS: We now have a one hour break for lunch, so please be back here around 1:15, thank you.

(Recess)

MS. PRITTS: Okay, good afternoon. I'd like to welcome everybody back from lunch. We're getting ready to start our afternoon session, so
please take your seats. Oh, thank you. That's my
technology expert. I have to have her with me
wherever I go. So our first panel this afternoon
is going to talk about -- specifically focus on
privacy and security issues. You've heard that
conversation sprinkled throughout the panels this
morning. I'm very glad that a number of the
people who are up here were able to be here this
morning and hear some of the things that are going
on that are very innovative in the field and kind
of change the landscape of what we've
traditionally thought of as medical information
and where it's held and how it's used.

So this panel is going to focus on, as I
said, privacy and security of identifiable health
information in PHRs and related technologies and
focus on consumer expectations and concerns, as
well of those of the attitudes of health care
providers and the industry groups to these same
issues, so we should have a broad range of
perspectives here.

I'm going to introduce the panel and
then we're going to have a little, you know, one
or two minutes of opportunity for the panel to
give a little background on themselves that I
haven't covered or their perspectives on things
and then we're going to go into our discussion,
which I think will be very interesting.

So first on my left here is Bob Gellman,
who I have known for very many years and who has
been in this area as long as anybody I know. He's
a privacy and information policy consultant in
Washington, D.C. He advises large and small
companies, for-profit and nonprofit organizations,
trade associations, government agencies, foreign
governments. Have you reported that, Bob?

MR. GELLMAN: I absolutely have.

MS. PRITTS: Okay, just checking. And
advocacy organizations how to develop, analyze,
implement and maintain policies for personal,
privacy and fair information practices. His
specialty areas include privacy policy for health,
including HIPAA, the Internet, the homeless,
freedom of information, and other information
policy areas.

As I was saying, everybody who works in this area in D.C. certainly knows Bob. He's the author of numerous columns, conference papers, congressional reports and scholarly articles on privacy and other information policy issues. And he, of course, has his own website which you -- will find on the handout here.

Next to Bob is Josh Lemieux, and I've had the pleasure of working with Josh over the years. I was a member, full disclosure, I was a member of the Markle Group that worked -- Connecting for Health Group that worked on PHRs a number of years ago now, and Josh was also on that panel. And what did we work on before that? I don't even remember. But I've known him for a number of years. And he is an expert on policy and technology for emerging personal health information tools and services. I will also say that Josh is one of the best writers I have ever met in my life, that's true.

MR. LEMIEUX: Just can't speak.
MS. PRITTS: Since 2004, he's managed Markle's research and policy development for electronic personal health records and collaborative efforts on patient engagement as a means to transform health care.

He's the lead writer and editor of the Markle Connecting for Health Common Framework for Networked Personal Health Information. In previous positions, he directed the launch of health benefit decision support tools at WebMD and led project teams creating interactive applications at WellMed, Discovery Channel, and Mayo Clinic.

Josh began his career writing for, and this is why he's such a good writer, he began his career of writing with UPI in Brazil and worked seven years as a correspondent for the AP, assigned at the Mexican border. So you and Bob probably have some international connections, is that right?

MR. LEMIEUX: I doubt it.

MR. PRITTS: You doubt it, okay. Next
to him is Lee Tien, he's a staff attorney for Electronic Frontier Foundation. And I've only made acquaintance with him, although I have read some of his work in the past. He's very well known, particularly in California, where he does most of his work.

He's a senior staff attorney with Electronic Frontier Foundation, specializing in free speech law and privacy law. As part of his policy work in electronic health records, he advises the California Health and Human Services Agency and its Office of Health Information Integrity, as a member of the California Privacy and Security Advisory Board Privacy Steering Team.

California is a state that we all look to for its innovations and how it approaches privacy, and some look to it with admiration and some look to the state with fear and trepidation.

Mr. Tien has published articles on children's sexuality and information technology, anonymity, surveillance, and First Amendment status of publishing computer software, and the
state secrets privilege. He received his undergraduate degree in psychology from Stanford University and his law degree from UC-Berkeley, where he also did graduate work in Program in Jurisprudence and Social Policy.

Our sole female member of the panel over there is Tresa Undem, who's the Vice President of Lake Research Partners. Tresa Undem has been with Lake Research since 2004, where she works with foundations, nonprofit organizations, and issue organizations on health and health care. She leads public opinion research on a variety of policy issues, including health IT and the use of PHRs, chronic illness, health care access and quality, and reform.

Ms. Undem specializes in conducting multivariate statistical analysis so the rest of us don't have to, to examine how messages and arguments predict attitude and behavior. Ms. Undem is the author of the California Health Care Foundation's Consumers and Health Information Technology: A National Survey, which was released
this April, and we are going to use her study as part of the framework for the discussion today, because it has a lot of very recent pertinent data for the discussion that we have on the table, and it's just an excellent study.

And last, but certainly not least at all, is -- can I call you Matt since we all do? Okay. Matt Wynia, who's the director of the Institute for Ethics at the American Medical Association. And he was named director of this Institute in May, 2000, so he's been there a while. And the mission of this Institute is to foster the health care of patients and the public by promoting the integrated place of ethics in medicine through research and educational outreach.

As director of the Institute, Dr. Wynia oversees the Institute's Fellowship and Visiting Scholars Program and a wide range of research projects on topics including physician's responses to utilization review and market pressures in medicine comparing the codes of ethics of medical
professional associations and the ethics-related
policies of health care organizations, exploring
physician professionalism and the role of
professionals in society and creating performance
measures for health care ethics, very interesting
cross-cutting issues there.

As the director of the Institute, Doctor
Wynia conducted the AMA study of the attitudes of
physicians to PHRs, another one of the studies
that we will be exploring a little bit in-depth
today. He also practices, in his spare time,
internal medicine and infectious diseases at the
University of Chicago Hospitals, where he's Chief
Clinical Assistant Professor of Medicine. So we
have a wonderful panel here this afternoon, and I
am honored to be able to moderate this panel. The
first thing we're going to do is, we're going to
let everybody have a few moments to give their
perspective on the issue and then we'll launch
into some more question and answer type
discussion.

So since we started here with Bob, I'm
going to start at the other end with Matt. And if
you want to take a couple minutes and tell us
where you're coming from, it will be really great.

DR. WYNIA: Sure, thank you. It's a
real pleasure to be here today. I'm honored to be
in this company. It was mentioned that I do a
little work at the University of Chicago in
clinical medicine there and infectious diseases.
And my primary patient panel is comprised of
patients with HIV infection.

So there are a number of reasons why the
topics today are of particular personal and
professional interest to me, as well as being of
interest sort of on an academic and, if you will,
policy basis, and this will show up in some of the
comments around the survey results that we found.

I guess by way of introductory comments,
I would say that, by and large, physicians, you
know, not 100 percent obviously, but many
physicians are really excited about the
opportunities that health information technologies
hold for improving communications with patients
and for improving delivery of important information, you know, from place to place within
the health care system and between patients and doctors.

With regard to privacy, obviously the confidentiality of patient information is a core ethical promise of doctors to their patients and of other health professionals to patients. And, in fact, I guess the thing I would emphasize is that given the nature of the health care system today, it's not a promise that any of us can keep without the help of everyone else on the health care team, including those who don't know about the ways in which information ends up in their laps, frankly.

The reality is, in my view at least, if you have personal health information in your possession, the reason you have it from someone else is because they trusted someone with that information, and that chain of trust ends up with you in possession of their information. And you may not feel like you've ever taken a Hippocratic
Oath, but you have, because you're holding someone's personal health information. So I'm very interested in ensuring that that chain of trust retains its strength and allows us to maintain that promise of confidentiality.

The other thing by way of background I'll say is, because this came up in the earlier discussion, and I don't think we're going to get a chance to talk about it a lot this afternoon, there are even with good privacy and confidentiality protection, still risks to some of the HIT tools that we're talking about, one of which -- some of the issues around the Blue Button download, for example.

We talked earlier about, one of the earlier panels, about the new security risks, and I would say one of the new security risks is patients inadvertently disclosing their information, downloading and leaving it on the library computer without recognizing that that is happening. So I hope either on this panel or the subsequent one, maybe we'll get a chance to talk
about that as a risk.

And then the other risk that we may not get a chance to talk about through the rest of the panel, so I'll bring it up now, is, any time you intervene in a care process or create a tool which intends to change the way care is delivered, there is a possibility that it will backfire and care will be harmed and patients will be hurt. And you don't have to be in clinical medicine for very long to come across a number of examples of things where we, in our hubris, thought it made perfect sense to put every post-menopausal woman on estrogen, or everyone with, you know, osteoporotic fracture on fluoride treatment.

You know, you can name dozens and dozens of things that made so much sense that we didn't even think they needed to be studied, they should just be implemented and done, and we ended up hurting people as a result. And I think there is the possibility that that kind of outcome could occur with some HIT interventions. So the ways in which we track the clinical implementation of HIT
interventions is of great interest to me and I think to many doctors.

MS. PRITTS: Thank you, Matt. Tresa.

MS. UNDEM: Yes, so again, I'm Tresa. I guess what I'll be drawing from mostly is our study, as Joy mentioned, from the California HealthCare Foundation, which was really an exciting study. It was the first one that had a nationally representative sample of PHR users, so that was really sort of the most exciting part of the study. And we got to ask a bunch of questions about users and non-users, as well, so I'm going to be drawing on that. I have worked with Josh in the past and the Markle Foundation on surveys, and Josh also has a really good grasp on public opinion on this issue.

I think I just -- a few things that really stand out to me, just from the perspective of a pollster -- well, first of all let me say, I don't know Bob, so that's how much I know about this topic. I'm much more like the public than the people in this room. I don't know half of the
acronyms.

And one thing I'll say is, the public,

number one, is clueless about PHRs. The majority
have no idea that they exist, know nothing about
them, so I think that's one thing we need to
always keep in mind.

Number two thing that really stood out I think from our study, and I think we'll get into
this, but privacy is an issue, but when we really
dug deep, and I did some statistical analysis, it
wasn't the number one barrier, it really didn't do
a lot in predicting people saying, no, I'm not
going to sign up. What did predict, what was, by
far, three times more powerful as a barrier to
signing up for a PHR was not thinking that --
thinking that I don't need this for my health
needs, that was far more important than privacy.
And it's not to say privacy isn't important, we'll
get into that, but that, you know, I reran those
regressions like four different times, I had a
colleague do it, I was really surprised, but then
there's other data, too, in the study and from
other studies that help tell that story, but that was a really interesting finding.

And I think -- and part of that relates to, you know, this lack of awareness of PHRs and all the concerns and privacy implications.

I think the other thing from the study that was really fascinating was the outcomes of using a PHR. We asked a bunch of questions about, has having your information online made you more knowledgeable about your health, I think fifty-six percent said yes.

Fifty-two percent were more knowledgeable about their health care that they got. Forty percent asked their doctor a question they wouldn't have otherwise asked just because they have a PHR. Thirty-eight percent felt more connected to their doctor. Thirty-two percent said they'd taken a step to improve their health as a result of having a PHR. So that was now -- that's self-reported, so those are probably inflated a little bit, but still really stunning. And we found that PHR users actually who are more
vulnerable, typically vulnerable populations,
lower income, more educated, more chronic
diseases, they were much more likely to benefit
from -- have these outcomes than other people. So
I would say those are sort of the three things
that really, you know, from my view as a non-
expert pollster, that was really sort of exciting
for us.

MS. PRITTS: Before we go on, I'm going
to take my executive privilege here and ask you a
question, which is, how hard was it for you to
find enough PHR users to actually field a national
poll on this?

MS. UNDEM: Yeah, I mean it's hard.
This was fielded last December and January, so
almost a year ago, and seven percent of the
population at that time reported having used a
PHR, and so we had to oversample, and so, yeah,
it's kind of a needle in a haystack right now.

MS. PRITTS: Thank you, Tresa. Lee.

MR. TIEN: Hi, so I'm Lee, and I was
going to say that I probably know less about
health privacy law than anyone else on the panel, but maybe, maybe not, but probably pretty close. What I do know a fair amount about, though, is privacy and privacy law in general, and that's where I'm coming from. What we know, our experience with privacy and privacy law online in particular in this country, but also offline, is, you know, people don't understand it, people don't know very much about it, people don't know what they are worried about, but what they actually should be worried about often has nothing to do with what they actually are worried about, because they don't know what the reality of actual information practices in the world are, and they have a misguided view of what companies or what the government can or can't do.

And so because they're secure often in believing that those risks don't exist, they're, therefore, unconcerned about their privacy, or they think they're making this very calculated choice about their benefits and their risks when, in fact, they're completely under, you know,
estimating the risks and the costs.

And so I guess the single -- the main point I want to make in my little intro is just that I don't think we do ourselves a whole lot of good looking at or paying attention to what patients say their concerns are anymore than I would say really judge my 14-year-old daughter's use of Facebook based on what her expressed concerns are, because the fact is, I know she has no idea what she should be concerned about, and I think, in general, we have no idea, or the American consumer has no idea about what they should be concerned about online. And I think that, you know, this week we saw the FTC's staff report on online privacy, and many -- some of the studies that we'll be talking about, talk very much about how poorly informed, you know, the public is about these things.

None of that is to say that PHRs and electronic health records in general aren't going to be good things and aren't things that we should have, but simply that we have to be -- really be
careful when we are designing these systems and
testing about what should or shouldn't be the
case, not to let the consumer's perceptions be the
touch tool, we actually have to be in touch with
the real risk so that we, as folks inside the
system, know and protect against those and not
just against what the public believes.


MR. LEMIEUX: It's really good on each
of your parts there, and it's going to be an
interesting discussion, because I definitely agree
that anytime somebody opens up a personal health
record or creates a new data flow, even if it's a
data flow to yourself by downloading information
from a patient portal or a health insurer site,
there's going to be, of course, new risk. It's
also a risk not to have your information. So if
you're going from care provider to care provider
and you don't have your information, that can also
be a significant risk to your health. And so
these things are complex and very interesting.

So in 2003, Markle started to study this
area fairly carefully, and we did it with the help of a great many people that are pioneers in privacy and Internet services, providers, insurers, lots of people who are eyeing this nascent concept of what is a personal health record.

And our approach has been to try to get those people together to agree on what the right practices should be in this space, and it's always going to be an evolving area and a moving target.

But we think that there is some foundational work done with the help of a lot of people here, Matt and Joy not in any way the least, to describe what the practices should be, whether a service is covered by HIPAA or not. In other words, whether you're covered by HIPAA or not, if you have a personal health record, it should have an audit trail, log, transactions of data transfers and things like that, that's just a good practice, and so we've tried to describe some of those things. And parallel to that effort of getting lots of different interests together in a
room to hammer out those types of practices, we've also surveyed the American public, and we've done it in a -- fielded six surveys since 2003, and the overall learning, if I were to put it in a couple sentences, is that, I agree, people do not think about these things, these are not top of mind issues, you have to present the idea to them in a survey, so we're measuring sort of anticipation or response, it's not experience.

But they like the idea. They do think that -- very strong majorities of the American public consistently have said that if they had their information electronically, they could do a lot of things to improve their health and health care.

And I think the California HealthCare Foundation Study this year also showed that, and they took the effort to actually look at personal health record users, and some of that concept, that idea that this would be helpful was borne out in that data.

The other thing is, they want privacy
protection, specific practices, and I'm sure we'll get into that in this discussion. We do have some new data coming out in the next couple weeks in a survey, and this time, after some experimentation with Matt on polling both doctors and patients, we are coming out with a survey that asks patients and providers the same questions about health IT, about meaningful use of health IT, about privacy, about information-sharing behaviors and expectations and aspirations, even about payment reform and some social networking, and so we do have some results that we can talk about during this panel.

There is in your handout, and for those of you online, it's the -- there's a document that's the feature document on the Markle.org website, M-A-R-K-L-E.org. So I look forward to this discussion.

MS. PRITTS: Thank you, Josh. Bob.

MR. GELLMAN: I've been in health privacy for more than 30 years. A good part of that period, I was on Capital Hill, and that's
more in the dim, dark, distant past. If anyone is interested in the history of failed attempts to pass federal health privacy legislation, I know it all.

More recently I did a report on PHRs and privacy for the World Privacy Forum, it's available at the World Privacy Forum website or through my website, and while I think the report is still very relevant, the issues are still the same, I think it probably covers what you might call the classical period of PHRs, with the model of PHRs as sort of the Microsoft model, of you know, you get a copy of your record and have somebody maintain it and it's clear that the world has evolved in a lot of ways.

My particular -- my number one hobby horse here, but by no means my only one, is commercial advertising-supported PHRs, which I think are essentially devices to transfer health records to marketers in a way that will raise health care costs.

There are many other models of PHRs,
clearly, and they don't necessarily all have the
same problem, but the issue of data leakage out of
all of these activities is still important.

I think generally the problems that we
face here are a lot of ways the same ones that we
face in a lot of other privacy areas, and the
theme here is borders. How do we find the
borders? What is health information, what is
sensitive health information? What is a PHR?
It's much less clear than it ever was. And how do
we make all of these distinctions in order to
establish rules? Whichever way you're going to
have rules, whether they're regulations or laws or
something else, you've got to be able to define
what it is you're doing, and it all seems to be
extremely messy and getting messier, and it's all
against the background of Internet activities
where essentially we have virtually everybody's
Internet activity is being tracked by numerous
different organizations that you've never heard
of, and you don't know that they are following
you, you don't know what information they have
about you, and all the health information is just
leaking all over the place into this, and we don't
know how to solve that problem, and we don't know
how to solve this problem, but we've got to try.

MS. PRITTS: Thank you. All right. So
with that as background, we're going to start a
discussion with a little context setting. Just
for those who are following us on a web cast,
these are some of the data sources of the surveys
that we're going to be speaking about today. And
for those of you who are here in person, this is
where you can go back and read the full stories.
We're going to start with Tresa. In your survey,
you asked a question about what's useful, what
people find useful in a PHR, so can you talk to us
a little bit about that?

MS. UNDEM: Yes, and I'm going to share
your thing. But, yeah, the most useful thing
among PHR users in a list of things we asked about
was making sure the information, their information
in the PHR was correct. And this is -- I do a lot
of -- probably 90 percent of my polling, research,
focus groups, surveys is on health care issues among patients and consumers.

And we, you know, most people think their quality of health care is good when you say, you know, when you poll in the survey, but the growing sort of concern among patients is that doctors aren't talking to each other, that there's drug interactions, because one doctor prescribes it, and you know, another one isn't aware of it.

So this wasn't really too surprising that this was the top thing, you know, just wanting to make sure everything is there, everything is correct. And that's also the number one thing that non-users would be interested in. And it's also just sort of a baseline, doesn't take a lot of work, it's sort of a baseline, you know, this is what I'd use it for.

Also it's checking lab tests and test results and things is another high one that's both for the PHR users was most useful, and for non-users, most interested in. And we've seen that for a number of years, that lab tests is one
of the highest ones.

MS. PRITTS: Is that what you found over time, Josh? Have you looked at that issue?

MR. LEMIEUX: Well, we ask about what do you think this would do to help you, not did this help you, so that's a very critical distinction.

But when we ask, for example, what would be the -- how would PHRs improve your ability, we found that 87 percent -- this is in the survey in 2008, 87 percent said, and the highest, was checking for mistakes or errors or tracking their health related expenses, and then 86 percent said, for each of these things, avoiding duplicate tests, procedures, keeping doctors informed of your health status, moving more easily from doctors.

And then in the 88 percent category, also, managing family member's health, getting treatments tailored to your health status. And so labs did come up, but we didn't ask about that recently. I'd say Tresa's data is a lot more relevant at this point.

MS. PRITTS: But what it sounds like is
that you did a survey of what people expected
would be helpful, and Tresa's survey said that
after people had started using PHRs, they actually
did find those same things to be useful. So
that's kind of a good check, to say that people --
the expectations in this area are probably, at
least at this point, being met in the benefit
side. So, Matt, turning to you, how do providers
view this, do they think that this is going to be
a useful thing, or we heard earlier that there
were some people, some docs, when approached with
a PHR, basically put garlic around their neck and
put a stake in their heart.

DR. WYNIA: So I mean as a baseline, a
couple things should be recognized. One is,
there's about 20 percent of doctors who say I will
never do anything electronic in my practice
lifetime.

MS. PRITTS: Okay. And how old are
they?

DR. WYNIA: Well, they're older.

MS. PRITTS: Okay.
DR. WYNIA: And it may well be that these are, you know, nearing retirement, and they're thinking, you know, it's just -- there are too many barriers to converting my practice, I don't intend to start emailing my patients now, I've never done it before, I'm never going to, I'm not even emailing my daughter, why would I email my, you know, so there's a group of people --

MS. PRITTS: Twenty percent is not insignificant.

DR. WYNIA: It's not insignificant, but there is a group -- so you've got to sort of set that group in your mind, not necessarily aside, but there is a cohort like that.

MS. PRITTS: Okay.

DR. WYNIA: The other thing as a baseline to understand is, doctors, like the general population, don't know a lot about this. Only around 10 or 15 percent of doctors have any meaningful experience with a PHR, ever.

MS. PRITTS: Really?

DR. WYNIA: So about 25 -- 30 percent
say they have ever seen a PHR, but it's in the 10, 15 percent range who have actually interacted with a patients' PHR in some way or another. So we're looking also at a --

MS. PRITTS: I'm compulsive about asking questions. So when you're looking at those doctors who -- were you just looking at the group who had an EHR or all doctors?

DR. WYNIA: All doctors; and when you start asking about having EHR, you then get into defining what you mean by an EHR.

MS. PRITTS: Okay.

DR. WYNIA: Many physicians believe they have an electronic record system of some sort. Whether that would qualify as, you know, the New England Journal article definition of an EHR, many of them probably don't.

MS. PRITTS: Okay.

DR. WYNIA: And so --

MS. PRITTS: Against that background --

DR. WYNIA: Against that background, right, not a lot of expertise, but there are, you
know, some of the same potential benefits are there. More, I think, doctors are interested in the ways in which PHRs might engage patients in their care and improve communication between patients and their caregiver team.

They're less convinced on a number of other markers, but I think it's more, you know, I assume everyone can see the slide, it's more that people just don't know. You can see the plurality of doctors in almost every instance except for the PHRs empower patients to participate more in their own care. The plurality usually says, I don't know. So physicians are at least willing to acknowledge that they don't have experience with these yet and they're not sure, so that's where we're at.

Ms. Pritts: Out of curiosity, did you -- they asked about the -- one of the things that the patients are really interested in is the ability to collect their information or check to see if it's correct.

Dr. Wyna: Did Josh put you up to this
MS. PRITTS: Well, actually he did.

DR. WYNIA: So it's a very interesting finding. It's a rare doctor, it turns out, who thinks that patients provide a meaningful check on the accuracy of the medical record. Most physicians -- and, by the way, we looked very carefully at this because it was a somewhat unexpected finding, given how common it is that patients say this is one of the expected benefits. So we looked, for example, at that ten or 15 percent of doctors who have regular experience using a PHR, so these are presumably doctors in systems where all their patients have PHRs, for example, they were equally, or just about equally uncertain or they didn't believe that patients were going to be going through the records, finding inaccurate lab test results. So in this instance, and I don't know, you know, why that is, it could be that those physicians with experience using PHRs have had patients come in with things that they thought were inaccurate,
that were not, in fact, inaccurate, and it ended up being a hassle for the doctor, and so when we asked them that question, not only did they say no, it doesn't work that way, they say it works the opposite way. I could envision that. It wouldn't take a lot of these doctors to have had one or two experiences like that.

MS. PRITTS: I think it'll be very interesting as we go forward for there to be some sort of objective measurement of whether it actually -- whether patients actually are finding discrepancies in the record or not.

MR. TIEN: Joy, could we ask Tresa if she has any sense from her survey why patients said that that ability to amend or correct was so important to them?

MS. UNDEM: We actually didn't ask that in the survey, the ability to. Josh, you've probably asked it.

MR. LEMIEUX: When we first started asking this question in 2004, we were surprised that the, I'd like to check my record just in case
message, was registered really quite high. When we were asking people sort of like, okay, which of these messages about a PHR is most persuasive to you, the sort of -- you got injured and you've got to go to the hospital and you need your records fast, that was the biggest reason. But checking for mistakes was very, very high. And then consistently over the years as we've asked it, there's just this perception that that would be a benefit on the part of consumers.

We didn't really focus group it to a level to see why do people feel that way. I guess, you know, there's the Seinfeld episode where Elaine is like what did you write in my record?

MS. PRITTS: For those of you who haven't seen that, you should really see it, it's very funny.

MR. LEMIEUX: So maybe it's just a, you know, and we haven't measured it across other sectors. Do you think that you could check the record in your, you know, mistakes in your
Department of Motor Vehicle record, you know, we have --

MR. TIEN: In other privacy areas, I mean certainly like with credit reports and stuff like that, it's very well documented they're full of errors, and so I mean it may just be picking up that people expect their official dossiers of all sorts to have errors in them and they want the ability to correct, and I was curious.

MS. UNDEM: And I don't think it's errors in lab test results or things like that, I think it's, you know, I think we all kind of wonder, for those of us who have doctors who are still writing down by hand, what the hell are you putting in my chart, you know, and do you have all the information, and all the right information, and are you hearing what I'm saying, and are you interpreting me correctly, I think it's probably more along those lines.

MR. GELLMAN: Another factor may be the rise in medical identity theft, which is a real problem.
MS. PRITTS: Okay. Well, those are all very interesting points, too. I don't think you were here earlier, Tresa, when Steve Downs was talking about that they're doing a -- RWJ is doing a study where they're actually having the providers furnish the patients with a copy of their notes at the end of the visit, to see how that goes on both sides, so that should be a very interesting outcome on that.

So we have both providers and patients thinking at some extent that these PHRs and this type of thing may be a good idea, but from what both of you said, not that many people are using them. And, Tresa, I think that you have some data here on the non-user's preferences towards the PHR source. So one of the things that I think is important in here is, what is it that they're looking for, who do they trust to give the information and that sort of thing, so can you tell us a little bit about what you found there?

MS. UNDEM: Yeah, and we found this over time, too, in other studies, and it's not
surprising, doctors, medical practices that you use, hospitals you use, that would be -- that's the number one preference. We've also found in this study, and I think it's the slide up there, the next is your health insurance plan, and some people might be surprised by this.

I think if we were to ask something like do you trust doctors with, you know, as a source for the PHR, do you trust health insurance companies, we would get a very different answer. But often when -- and we see this is other issues, that people tend to rate their own health plan, you know, more highly and trust them more than insurance companies in general, just like I hate Congress, but I like my member of Congress type of thing.

And then after that, it's government agencies and non-profits and employers, and then sort of at the bottom is the private technology companies, and I think, Josh, that's pretty consistent.

MR. LEMIEUX: Yeah, we ask in these
questions and found the doctors at the top and then actually insurers second. But the way that we asked the question was, if this were offered, if this type of service were offered by this type of entity, would you be more likely to use it or less, or the same, you know, is it neutral, and the bulk of people, more than 50 percent said neutral.

So it's too big -- it's not right to generalize that only the doctor supply PHRs are trusted and the others are not. I think people -- this is an experimental new model, and there isn't a lot of experience, and a lot of people are reserving judgment on it.

MS. PRITTS: So, Matt, what do -- in your survey, you did kind of a flip of that, looked at the flipside of that as to what the provider -- what source of information the providers would trust the most, right?

DR. WYNIA: Yeah, and I think, again, by way of background knowledge for this question, this question came towards the end of a survey, it
was about a four-page survey, and so you can kind
of think of surveys sometimes as educational in
nature, and so by this time we had asked a number
of questions about the accuracy of the information
that might be in a PHR, so now we get to the
question of, if a PHR were offered by the
following, would you trust it.

    MS. PRITTS:  Right.

    DR. WYNIA:  And I guess, incidentally,
Bob, we did ask in a separate question, not on
this chart, whether you would be willing to use a
PHR that contained advertising, and only 8 percent
of doctors said they would be willing to use a PHR
that contained advertising. Now, whether that is
reflective of what might happen in real time, we
don't know, but that's what people said.

    Otherwise, I feel like our results are
somewhat similar to what we've heard so far from
the consumer community, which is to say
physicians, too, are more likely to be trusting of
a PHR that's run by their own group or the
hospital within which they practice.
Next would be a specialty society or some other professional association, the AMA State Medical Society, something like that. Third would be a government agency, Medicare or Medicaid, and that's how we said it was a government agency such as Medicare or Medicaid. We then said a health plan such as Kaiser or Aetna, so those were the example categories, and then Google or Microsoft.

MS. PRITTS: In fact, what we heard from our earlier panels is that Google -- well, I don't know about Google because they weren't here, but Microsoft actually works very much hand-in-hand with some of these other organizations, so it's really hard to make that distinction at this point, isn't it?

DR. WYNIA: Yes, and what we said is a commercial entity such as Google or Microsoft, you know --

MS. PRITTS: Right.

DR. WYNIA: -- for what it's worth, that's how the question was framed.

MS. PRITTS: Okay. We also -- so that's
a theme that came up a couple times today, or repeatedly today I would say, is the trust of, you know, trusting the source, trusting that the information would be accurate. Tresa, in your survey, there are also some other -- you asked about other potential barriers to using a PHR, and would you talk to that a little bit for us?

MS. UNDEM: Sure. Well, first of all, I think the number one barrier is not knowing it exists. So --

MS. PRITTS: That's a significant barrier.

MS. UNDEM: Yes, that's a very significant barrier. So we asked in our survey a number of questions, worry about the privacy of my information, 75 percent agree. The strongly agree is less, I think it's about 35 percent. We asked about whether they think they need it to handle their health needs, it might cost too much, I don't like computers, it might take too much time, these were the main barriers we asked about.

And then, again, what I did was, I ran
regressions on a post measure that asked how interested are you in signing up for a PHR. And regressions basically look at the -- is it really statistically correlated with wanting to sign up. So people who say, yes, I'm worried about privacy, but that has nothing to do with whether they're going to sign up or not. So regression helps tease that out, and that's where we found that really the number one thing is feeling that I don't need this, and that's the 61 percent. So that was -- in fact, all of these barriers were more significant than -- had a more significant relationship with not wanting to sign up than privacy.

MS. PRITTS: So let me ask you this, and I'm going to throw this out to the table in general, what it sounds like is that there are a lot of people who don't find the PHR concept to be very useful in the way they're looking at health care, and if you added on top of that some concerns about privacy, as to whether that information they would put up there, what kind of
effect do you think that would have, Bob?

MR. GELLMAN: Well, I don't know, you're

sort of adding ignorance to ignorance. I mean

people don't really understand what the privacy

rules are, and people may not -- I don't think --

I'm not sure I understand what a PHR is anymore.

There are just so many different flavors of

things, so I don't know how you put that together

and draw any kind of, you know, in another way,

it's like you talk to -- the panel earlier talked

about trust and do people have trust, well, trust

is very nice, but that has nothing to do with

knowledge, you know.

I've seen surveys of government

agencies, do you trust government agencies to

handle your records, and I've been doing

government privacy for a long time, I have no way

of assessing whether they're doing a good job.

When we ask people in the public, who presumably

make perhaps occasional exceptions know less than

I do, what are you learning here? What does it

mean? I don't know.
MS. PRITTS: Josh.

MR. LEMIEUX: I kind of disagree with the first part of the question. We're living in an information age where people see the ability to connect to information, connect to services, log on to get things, make transactions. You know, I challenge anybody to just ask a stranger about, you know, hey, if you had your records online, do you think that would be helpful.

I think people understand that the possibility would be helpful. Now, converting that to action has certainly been a lot slower than many proponents would like, but the fundamental concept is not a difficult thing for people to understand, I think it's more sort of opportunity.

Now, when it gets to privacy, rather than asking whether people are concerned about it, we've kind of taken the approach of, well, which of these types of protections do you think are most important.

MS. PRITTS: And what do they say?
MR. LEMIEUX: Well, when we ask things like should you be able to review who has had access to your record, audit trail, should you be able to -- should you be notified if there's a breach of your information, should there be a mechanism to request a correction of information, should there be an ability to exercise choices over how your information is used. Eighty percent to 70 percent range people say, yes, that's important. What's interesting also is, 80 percent to 70 percent range of doctors also say those things should be important for people, and we ask it specifically in the context of meaningful use.

DR. WYNIA: Further proof that doctors are people.

MR. LEMIEUX: Very good, yes, we confirmed that, we confirmed the hypothesis. So very large -- and if you look at the disagreement column, and these are in this handout here, very few people disagree that those four policies, those practices are unimportant. Let me say that again. Almost nobody says that they're
unimportant, a vast majority say that they're
important in both groups.

MR. TIEN: If I could throw something in
here, what we, again, this picks up something that
may end up not being very important or its impact
is ambiguous, because on the one hand, people tend
to believe that those kinds of protections
actually already exist. The studies we've shown
of things as mundane as, you know, pizza delivery
or charitable donations and product warranties.
People believe falsely that they have all these
c kinds of rights, and basically, you know, they
don't. And not only do they believe that they
have these rights under law, they apparently
believe that these companies aren't doing any of
the things that they shouldn't be doing, even
though the law says they can.

And so there's a whole sort of happy
ignorance about what's going on in the background
of the data world, which I think makes it really
hard to sort of figure out what these things, you
know, what they really mean for.
So the other half of it is, if we're talking in surveys about privacy as a very general sort of concept or trust or even, you know, health information, you know, we already talked today about sensitive health information, and, you know, if we don't know when people are talking about what's important to them, whether or not they're thinking about, I'll use the example of my tennis elbow, on the one hand, or whether they're thinking about, you know, their daughter's, you know, anorexia, or some kind of a mental illness, or HIV status or whatever, you know, their perception of what the risk of some kind of sharing or some kind of electronic environment may be, you know, very, very different, which is one of the reasons why this morning, from the earlier panels, we were talking about this going social and this whole sort of sharing community thing, and I'm going, oh, I was, you know, I learned something, I wasn't aware of this -- what people were doing in this era with PHRs, and that struck me as being a very powerless sort of thing to be
doing given how little we know -- any of those
patients know about how information is going to be
accessible.

So, you know, and there are legal -- the
last -- because the law itself is so unclear, you
know, even leaving HIPAA aside, which no one
really knows about, I mean I think a lot of people
do believe and know about things like the
doctor-patient privilege; whether they realize
that the moment they hand information to someone
who's not a doctor, that they waived that
privilege, and it just doesn't exist anymore, and
if the belief and the privilege is part of what
makes them believe that the law protects them, and
they don't realize when they waive it and how,
even if it's coming in from a doctor into their
personal health record, but because the personal
health record is held by a non-provider,
therefore, the privilege is gone. I mean I'm just
not sure how anyone has any, you know, comfort in
what people think about this.

MS. PRITTS: Okay. So you raised a new
point. Tresa, did you want to say something?

MS. UNDEM: I just wanted to say that,
you know, when we did this analysis, just to
repeat what Lee has been saying, and Bob, too, the
public doesn't know anything really about privacy
and what's going on and what -- how their
information is shared, they don't know anything.

So at this base level of no knowledge,
they're not concerned about privacy, okay, so
that's what I was making the point, with no
knowledge, they're not concerned about privacy.
What's really going to make them be interested is
whether they need this, whether it's useful.

So when you bring in -- first of all, we
can't expect the public to know about this really,
and they're not going to learn about this. I
mean, they just -- we don't have time to learn
about every single issue on the planet. So we
have, you know, family anyway. So in surveys when
we do say, you know, we even asked in our survey,
so would it be okay to share your information if
your name is not attached, your address, your date
of birth, social security, you know, whatever, is
that okay to share your information, are you
comfortable with that, only 31 percent say yes.
So --

MS. PRITTS: If -- I wouldn't call it
de-identified, but when the information has been
what I would call anonymized, people still were
not comfortable with it?

MS. UNDEM: Right, right; and also, I'd
just add from, again, from polling, when the
public lacks -- it just lacks information, the
question wording really matters. So I know a
recent poll asked something like, do you think
doctors and health systems should be allowed to
share or sell your sensitive information without
your consent, and 97 percent said no, not a really
great polling question, by the way, when you get
97 percent saying no, and who are those other 3
percent?

MS. PRITTS: Yeah.

MS. UNDEM: I don't think they read the
question right or something.
SPEAKER: They said if I got a cut, right? No.

MS. UNDEM: Right. So there's, you know, and it's just complicated. It's when you ask them, okay, but here's what you get, in exchange: We get better quality care, we get, you know, we learn about the best treatments, and they're more willing I think. And I think in terms of trust, when you don't have knowledge, that the trust is the proxy. They're not going to get the knowledge we want them to have, that Lee has, that the experts have, so trust is a proxy, and for PHR users, that was one of the things that reassured them, was sort of the trust in their doctor or the trust in their health plan, the reputation of their health plan.

MS. PRITTS: Josh, you had a point?

MR. LEMIEUX: Well, just on this very issue of personal data and supposedly, you know, de-identified data. We asked, in the context of the Federal Stimulus Program, which policies people -- doctors and patients -- think should be
important requirements in order for that money to be well spent, and one of the policies we asked about was that the government could not collect health information as personally identifiable for health information technology or health care quality improvement programs.

Sixty-five percent of the public and 75 percent of the doctors said that that's important, that the government not be able to collect personally identifiable information. But when we said, if there are safeguards to protect identity, 77 percent of the public is either somewhat or very willing to allow their composite information to be used. So, again, people don't know all the ins and outs of stripping identity from information, which is actually a very, very complex area. But at the conceptual level, they want to be able to help, they see that there's public interest uses that are good, and as long as they feel protected, they have consistently over a couple surveys shown to be willing to -- that their information be used as long as it's
de-identified for many public interest uses,
including quality improvement.

MR. TIEN: If I could throw in one more
point, which is actually Bob's point which he
mentioned to me at lunch, about the fact that it's
not just about you, right. Bob, do you want to go
ahead and make the point?

MR. GELLMAN: Go ahead.

MR. TIEN: Well, I mean, I started with
the idea, coming from a state where there are a
lot of direct-to-consumer genetic testing
companies. And so one of the things, interesting
things about genetic data, of course, is that it's
not just about you, it's about your entire family
and everyone you're related to.

But once you start looking at how much
we know about ancestry and what not, then we
really almost -- many of your health conditions
end up being things that are going to, you know,
if they know that I have, you know, high blood
pressure and it has a genetic component, then
people that I'm related to may be at higher risk
of this or that. And so in really, in many, many cases, even though we're thinking about an individual making a choice about whether or not to disclose or share, they are really making choices that effect, you know, everyone they're related to, and we don't have really a -- we certainly don't have a legal framework for dealing with that kind of problem.

MR. GELLMAN: Can I add a word on that, and just the obvious point that once your medical information is out somewhere in the marketing world, it's out there forever, and it won't -- I don't think -- if it's not going on today, it will be tomorrow, that marketing companies will have medical family pedigrees with all of the information that they can scarf up from all of these various sources about everybody and they're going to use it for marketing, and you will get messages that say your family is at 20 percent greater risk for, fill in the blank, than anybody else, buy our product, it's guaranteed to come.

MS. PRITTS: Matt.
DR. WYNIA: I want to go back and reinforce a point that Lee made just a minute ago, which is the legal frameworks around privacy may or may not be clear to most people, I suspect are not, but the ethical framework is perceived to be very clear. And it gets back to where I started the afternoon, around -- to my mind, because of that, we're not really that interested in the matter of trust, per se, we should be interested in the matter of trust worthiness.

We know we have trust, doctors, the health care system, by and large, we know we are trusted, and we're trusted to do things which we may or may not be doing effectively, in part because of the partnerships that we're forming in order to try and do our work more effectively and so on, but we have this trust, we have to do everything possible to merit that trust.

And whether, you know, that may or may not be reflected in public opinion polling, but it's still our job, that's the policy challenge.

MS. PRITTS: Right.
DR. WYNIA: It's not to say, oh, we've got the trust already, let's go ahead and take advantage of it, it's we have trust now, what can we do to make sure we warrant that trust.

MS. PRITTS: So you're making -- I hear very clearly the distinction you're making is that we hear the - we've heard this theme of trust, we see that, from some of the surveys, that people, when they kind of trust the institutions, they think that this is a more reputable resource for the information, and someone -- they're more willing to have hold their information, and your point is, maybe not, that we can't just rely on that individual to have that trust, you have to have the person who's having the information behave in such a way that they actually -- that trust is actually well placed?

DR. WYNIA: Yes, right.

MS. PRITTS: Okay. So I would like to turn a little bit to some of the particular issues that we talked about a little bit, we touched on a little bit earlier. I think I'm going in the
wrong way. Here we go, there's the trusted
organization there. I'm just going to flip here
to where -- okay.

So these were -- Tresa, when you did
your survey, I think this shows one of the things
that we were talking about here earlier, which is,
that it was the trusted websites that people who
actually were using PHRs, that made them feel
comfortable. And what Matt is saying, maybe
you're feeling more comfortable than you should be
feeling. But some of the things, and password
protection, that made people feel a little bit
more comfortable. The secure website made people
feel comfortable. And can you explain a little
bit about what --

MS. UNDEM: Yeah, the HTTPS or the lock
symbol.

MS. PRITTS: So people are familiar with
those and they have an idea what they mean?

MS. UNDEM: This was an open ended
question, so we said what made you feel that your
information was safe and private, what reassured
you, and so those were the secure ones, that's where people said, because I saw the lock symbol or the HTTPS.

MS. PRITTS: And I was surprised when I saw this, because the site's privacy policy and HIPAA did not rank very high at all.

MS. UNDEM: Yeah.

MS. PRITTS: And nobody else is surprised by that, okay.

MS. UNDEM: I mean it's alarming really. I'm scared now that I'm learning more from these people. I mean one in five weren't worried at all. And then to just say, you know, 15 percent said, oh, because I had a password and user name, and then 15 percent say, or 16, whatever it was, that it was a secure website. I mean there's -- and yes, I think Bob and others have data about whether people read the privacy policy and whether it matters at all.

MS. PRITTS: I think so. I think, Lee or Bob, have you looked at the, I think it was the Hoofnagle study at all?
MR. GELLMAN: Chris Hoofnagle at Berkeley did a study, and basically what they found was, people think that if a website has a privacy policy, that that means they can't disclose their information to somebody else, just because they have a policy, not the content of the policy. So there's tremendous fundamental misunderstanding on the part of the public.

MR. TIEN: Which I think is also shown by the answer about HTTPS and the locks, because what it tells you is that the threat -- to the extent they know what those things mean, they're only looking at a very limited threat model, right. If they know what SSL is, they're saying, oh, someone's not snooping on my transaction, or, you know, there's a lock, oh, it's secure against the unauthorized, you know, outsider. But obviously, the biggest hole in all of this is, well, when the person you're handing your data to decides to share it with someone else, and, of course, there's no piece of technology other than encrypting the whole record in such a way that the
holder can't actually get to it that's going to prevent that, and so it just tells us that they don't know what to be worried about.

MS. PRITTS: I think it was from the Hoofnagle study that said that people don't even read the privacy policies. Is that right?

MR. TIEN: Well, that one is in a lot of studies.

MS. PRITTS: When they say they don't read them, do you have a rough percentage of how many people have actually read them?

MR. GELLMAN: Whatever it is, it's a really small number.

MR. LEMIEUX: And it's important not to conclude from that that those policy statements aren't unimportant or that the plain language summary that was talked about in the previous panel are unimportant. In fact, the extremely important thing to do, for an organization to think about what they're committing to, and those commitments are enforceable by the FTC if somebody violates them and it gets to that level. And so
state attorneys general --

MS. PRITTS: But don't you think people need to know -- people need to read them first? So it seems to me that you have a disconnect. If you have something called a privacy policy and nobody is reading it, there must be something there that -- some action needs to be taken so that people would maybe read it.

MR. TIEN: Well, I think they're picking up two different things. They're picking up one, which is what we talked about before, the default, the idea that they already believe that, absent anything else, the law protects them in a lot of ways, and that's one of the Hoofnagle study that, like I said, with the pizza delivery, et cetera, et cetera, they just don't think that companies can share because that's what the law says, A, and --

MS. PRITTS: A lot of us don't know what the pizza delivery thing is, so can you explain it a little bit?

MR. TIEN: Oh, it's like, you know, you
call Domino's up, right, and you give them your credit card and whatever information, they just assume that the law prohibits Domino's from doing anything with that data other than to deliver your pizza, which is completely not the case. But -- and so my point is the default level of protection that the law sort of lays -- puts down for everyone, the consumer gets wrong. And then second, they think that the fact that a company has a privacy policy means that they've also undertaken some additional privacy protections, and so the -- I mean, Hoofnagle's conclusion in that paper is that the very use of the phrase "privacy policy" is essentially -- ought to be prohibited or treated by the FTC as an unfair, deceptive and misleading trade practice, because it is known empirically that people actually think they're protected, no matter what the privacy policy says.

So, you know, Josh is absolutely right, I mean it is important what they say, and we do want them to know, and it does provide --
MS. PRITTS: But there's an important step before you get there, which is somehow signaling to people that this is not what you think it is.

MR. LEMIEUX: And it's why in the Common Framework we focus so much on the concept of independent consent, that there's an umbrella terms and conditions you sign on when you sign onto a service, blah, blah, blah, yeah, I'm not going to read that, click, and I'm in. But when the action that is being asked is to actually move my information to, you know, disclose it to a third party, or some type of activity that is unexpected by, you know, a normal person or a reasonable person, then the choice mechanism should be discreet and specific and should make clear what is happening in a concise way right at the decision-making moment, and so that's another practice, you know, best practice protection that helps, because we can't rely on the umbrella statement.

MR. GELLMAN: People will -- I don't
think there's any reason to expect people to read most privacy notices. If you just think about the HIPAA notice, it's all there, people will read it when it makes a difference to them, which is less than 100 percent of the time, most of the time it doesn't matter to you.

When you run into an issue, when you have a dispute, when you have a problem with payment of a bill or whatever, then you're going to look to see what your rights are, and then you'll read the notice, and that's perfectly all right.

MR. LEMIEUX: And public opinion, just on this question, we asked very clearly, do you agree or disagree with the following statement, no matter what I signed -- what I agreed to when I signed on, do I want to be asked specifically whether my information is going to a third party or being sold, and 84 percent of the public -- maybe 85 percent of the public said yes.

MR. TIEN: And the FTC staff report that came out this week on online privacy, one of the
points that they made was that they are -- they
want to push harder for what they call just in
time, you know, sort of notice, because, again,
they also see as a general matter that the blanket
general in-advance consent that sort of gives away
all your rights just isn't enough to protect
anyone.

    DR. WYNIA: And the other thing that
makes this all kind of moot is, if you're given
notice, but you actually have no choice, right, if
it's the pizza shop, I can choose to go to another
pizza shop. I can stop using Domino's
conceivably, right. I could, although the new
crust is good.

    But I'm already seeing my doctor, my
family is already seeing my doctor, I've got
relationships with the clinic staff, you know, and
now they've got a new PHR that they're rolling
out, and I'm going to click, and it really doesn't
matter whether I read it or not because I have to
trust them, you know, otherwise it's going to
affect the quality of care that I'm receiving.
So, I mean, there are places in medicine where consumerism works and there are places in medicine where the whole consumer model, where they pretend that we have, you know, wide open choices, and there's easy entry and exit into the market, and free, you know, access to switch providers just doesn't work.

MS. PRITTS: So how do you think -- there was a little bit of talk about accountable care organizations at some point this morning I think. Maybe that was just in my world, but --

DR. WYNIA: You were thinking about ACOs.

MS. PRITTS: Yeah, I think I was. How do you think that's going to play into this?

DR. WYNIA: Well, I mean it's a great question, of course, because the regs are being written right now. But I hope that, in the end, we see accountable care organizations that further this notion that everyone in contact with the patient's personal health information understands their ethical, if not their legal obligation, to
treat that information as though it were entrusted
to them just as it was entrusted to the doctor in
a closed exam room, where that patient assumes
that the doctor is not going to, you know, turn
around and sell the information to someone.

They, you know, when you go to see a
doctor, you have to make that assumption or you
can't have an effective patient-doctor
interaction. And if some additional member of the
health care team now gets access to that
information, they got it because the patient
trusted the system, the doctor and the system, and
we've got to be worthy of that trust.

MS. PRITTS: Okay. There are two other
points that I want to make sure that we get to in
our last few minutes here; well, actually there's
three. So the way you were describing this, that
was within the context of a patient- and a
provider- oriented PHR. It is a little bit
different, though, when the PHR is what I would
call disassociated from a health care practice, or
I guess even a health plan, and in those cases,
people actually do probably have a choice as to what they want or what service they could use a little bit more.

MR. LEMIEUX: This may be where the Blue Button issue comes in, as well.

MS. PRITTS: Yeah.

MR. LEMIEUX: The notion of downloading your information to a separate site, which could then be manipulated in a variety of different ways.

MS. PRITTS: And is it in that context where it's even more important that the information as to who it can be shared with and -- is that even more important there or is that not -- do you see that not being the case?

MR. LEMIEUX: Well, you know, we always approach privacy as not only protecting the information, but also giving people access to it. Getting access to your information is a component of privacy along with transparency and choice mechanisms and a lot of the other -- and enforcement and redress and error correction and a
lot of these other things, that's why privacy is so difficult to define, no one activity protects it, no one definition defines it, it's multifaceted.

But in terms of the Blue Button, you know, we -- the idea that you can download your information just for your own possession is a fairly powerful idea. Seventy percent of the people in our new survey, the public said that they thought that patients ought to be able to do that, and sixty-five percent of doctors said that they thought that patients ought to be able to download their information.

And we've seen, you know, with the proliferation of things, like iPhone apps, iPad apps, you know, just the power of innovation when there's lots of people that can create value added services on top of the data, we don't want to shut that off.

MS. PRITTS: Can I ask you a question? So when you do the download, is it a secure connection, is it encrypted?
MR. LEMIEUX: Yes, in order to get the
download, according to, you know, the practices
that I think organizations that have implemented
it, including the VA and CMS, is, you get it, you
log in, so you're entered into a secure
environment.

MS. PRITTS: Okay.

MR. LEMIEUX: And then you download it
under SSL and things like that, and there are even
other mechanisms to protect it further, including
things like those annoying captchas, those are the
little squiggly lines that can help determine
whether or not the download is being requested by
an actual human or some type of automated process
and things like that.

And so we have a paper on this that is
just sort of trying to plow some of this ground,
and a lot of people, you know, 50 different
organizations, you know, signed onto it, so we
think it's a good potential for innovation, not
without risks, but certainly, as I said at the
very beginning, not having your information is
also a risk.

MS. PRITTS: But it sounds like the encryption at least avoids some of the problems that we've been reading about lately in the Wall Street Journal, with the data being essentially scraped as it goes through the Internet by data aggregators, and if you didn't have that kind of a connection, it could readily happen, where people could be -- organizations could be scraping your information and adding that to their data profile of people.

MR. LEMIEUX: Yeah, PHRs have to be behind a secure socket layer if they're using, you know, real medical data, but we also can't preclude models like PatientsLikeMe, which are entirely different models.

MR. GELLMAN: But it's worse than that. I mean if you get your medical record and you sit on your PC and you go through all the pieces of your record and you put it all into a search engine, the search engine has all of your requests, and they know your entire medical
history now, and it’s good, bad, or otherwise, but
that’s what happens.

MS. PRITTS: Okay.

DR. WYNIA: It may come to you securely,
but once you have control of it, with control
comes responsibility, and it may or may not be the
patient sitting in the library having downloaded,
you know, their entire medical record onto the
library computer, or you know, on the subway
downloading it onto their Smartphone, understands
what happens when that now gets imported into an
app.

MR. TIEN: Well, we know they don’t
understand, I mean --

MS. PRITTS: Yeah, that’s right. I
don’t know about you, but I don’t know that I want
to know. Before -- we only have a few minutes
left here, and one of the issues that I wanted to
conclude with was that, well, I go to a lot of
conferences, and I am always, always told, well,
don’t worry about it because this younger
generation, they don’t care.
Privacy concerns are waning, you know,
in another ten years this is not going to be an
issue. So I'd like to toss that on that table and
then stand back and get some reaction to that and
see what you think about that issue.

MR. GELLMAN: There are studies that
seem to undercut that, one done by Chris Hoofnagle
out at Berkeley, that basically found, A, that
kids know less about privacy than adults, B, that
kids actually make greater use of some of the
privacy controls than adults do, partly because
perhaps they understand better than adults do, but
I don't think the attitudes of kids are
particularly interesting. Kids go out and get
rip-roaring drunk all the time, they text while
they drive. I don't know that we need to change
our habits or our laws to suit what kids are doing
today. Kids don't always know what's in their
best interest.

MR. TIEN: Or maybe to put it more
bluntly, when I was a kid --

DR. WYNIA: More bluntly?
MR. TIEN: True, you know, it's -- and then, you know, you grow up. So I mean, I think that there is -- I think there is a real -- I think the idea that we see a generational difference is because every generation sees a generational difference.

And, you know, there's a great social psychologist, danah boyd, at Microsoft Research, who does an enormous amount of study of social media and how youth operate. And, you know, she starts out from the point that you have to remember that kids, certainly the teenagers, are -- live in -- they exist in the most highly surveilled sort of situation of any kind of person in say, at least in, American society. They're constantly being watched by their parents, by their siblings, by their teachers, et cetera. They have as little privacy as anyone except for maybe someone in a prison or something. And so we shouldn't --

MS. PRITTS: She's been talking to my daughter, hasn't she?
MR. TIEN: Maybe; and we shouldn't be surprised by the fact that 14, 15, 16 year olds have sort of funny attitudes about privacy compared to folks who are able to actually live on their own. And at the same time, danah's research shows that they cope and they use all sorts of tools in order to try to protect privacy, to communicate in certain ways using the tools that are available to them in social media.

I mean it's a different issue as to whether or not they're effective, given that even experts that I know on Facebook privacy settings constantly find that they just shared information they didn't intend to. And I mean that's people who have, you know, who know it well enough to do videos explaining how to change, you know, personalization, and they still screw up.

So for teens to fail shouldn't be a surprise. But the point is that they still care. And, you know, danah's big overall point is that what we are seeing in the social media world, and a lot of the online world, is a big shift in
privacy, right. In the old days, we were private by default, public by effort, and so you had to work to actually get something out, and if you didn't do anything, you know, it stayed in one place. Today's world, especially in the social media world, it's public by default and private by effort.

So whatever effort is required for something, there's going to be less of it, and that's sort of the environmental condition for all of this, and I think that's as true, you know, in the, unfortunately, in the electronic world for health records as it is in the rest of the Internet, and that's why, you know, I sound like sort of a grumpy person about these privacy issues on these things.

MS. UNDEM: Not as bad as Bob.

MR. TIEN: Only almost?

MS. PRITTS: Okay, I think we're at the end of our session. I want to thank you all, this has been very interesting and enlightening. So we will now move on to - if we can thank this panel,
we'll now move on to our last one of the day.

I am sorry, we're taking a five-minute break and then we'll be back for the last panel.

(Recess)

MS. PRITTS: Can we please sit down so we can get ready for our final panel for the day.

Thank you. We are getting ready now for our final panel of the day. Our final panel is actually two subpanels, which I will let Leslie explain a little bit. How is that, Leslie? Is that fine?

The two panels will be moderated by Leslie Francis who is sitting here in the middle because she's much more comfortable there than she is over here at the podium with her back to half of the audience, so she is more considerate than the rest of us, too. This last panel is going to speak on the perspectives of privacy and security requirements for PHRs and related technologies. And at one point we had called these regulations, but we concluded that that was probably too narrow for focus and we used the term requirements very intentionally here. This panel is divided into
two and it's going to address the need for privacy and security requirements for PHRs and related noncovered entities. The second part will provide a forum for different views on the appropriate regulation, if any, or other requirements that should be applicable to non-covered PHRs and related service providers and technologies.

But the first subpanel we are very fortunate to have with us, representatives from some of the major, the committee, and the major agencies that actually do regulate in this area who are going to give us a little bit of background. We're also fortunate to have with us Leslie Francis who has been with us all day as the moderator of this panel. Leslie is a Distinguished Professor of Law and Philosophy and the Alfred C. Emery Professor of Law at the University of Utah. I know Leslie from the National Committee of Vital and Health Statistics, where she is the Co-Chair of the Privacy and Security Subcommittee on that panel, where she has given a lot of thought and consideration of these
issues. Leslie holds an adjunct appointment in Family and Preventive Medicine in the Division of Public Health, Internal Medicine and Political Science also at the University of Utah. She received her B.A. From Wellesley and she graduated with high honors in philosophy, so she's not just a lawyer, she's a philosopher, which is a very nice combination. She received her Ph.D. in philosophy from the University of Michigan and she served as a law clerk to Judge Abner Mikva of the United States Court of Appeals for the District of Columbia Court. A lot of us in the District remember Judge Mikva very, very well so that must have been quite the experience. She was appointed to the law faculty in '82 and she teaches and writes extensively in the areas of health law, bioethics and disability and we are fortunate enough to have Leslie working with us under subcontract with MAXIMUS on collecting some information and doing a study on PHRs and noncovered entities over the summer, which we are still in the process of -- and the study is still
ongoing and this information that we have gathered
today will become part of that. Leslie, I will
now turn it over to you. Thank you.

DR. FRANCIS: Thank you very much. I
want to thank all of you for staying with this for
what I hope will be as rich a panel as all the
others have been so far today. So for the first
part of this last session, our goal is to
understand from these panelists what the current,
and I'll call it regulatory for this part of it
because what the current structure is of the
requirements that apply to personal health records
and related entities. I have with me three
panelists. The first is Adam Greene who is the
Senior Health Information Technology and Privacy
Specialist at the Department of Health and Human
Services in the Office for Civil Rights. Adam
advises OCR on the application of the HIPAA
Privacy Rule in the area of health IT, including
electronic health records, personal health records
and health information exchanges. Additionally,
Mr. Greene represents OCR in Department matters
related to health IT, such as by acting as a HIPAA Privacy and Security Rule subject matter expert to the HIT Policy and Standards Committees. So that is Adam, here.

On my right is Loretta Garrison, who is Senior Attorney in the Division of Privacy and Identity Protection at the Federal Trade Commission. Loretta is here.

And on my far left is Joanne McNabb who is Chief of California's Office of Privacy Protection. You may have heard already today that California, among the states, is a leader in health privacy law and is the state that has, in state laws, specifically addressed personal health records and we'll be hearing about that from Joanne as we proceed.

So what I want to do with the panelists in the beginning is start out by setting the stage. I'm going to ask Adam to discuss what the Office for Civil Rights does, its scope of authority, the approach it takes to PHRs and the approach it takes, more generally, to the
regulation of health information. Then we're
going to ask Loretta to answer the same question
about the Federal Trade Commission. And then
we'll turn to Joanne to give us an overview of
what California is doing with respect to the
regulation of PHR providers.

This is somewhat technical material and
I think each of the panelists is going to take a
little more than the 2 minutes that the sets of
panelists did with the primary questions in the
other panels. So without more ado, Adam?

MR. GREENE: Thank you, Leslie. So, the
Office for Civil Rights, amongst its other duties,
administrates the HIPAA Privacy, Security and the
HIPAA breach notification rules. Now as has been
alluded to earlier today, HIPAA jurisdiction does
not follow the data like some other laws do.
Rather, HIPAA jurisdiction, our Office's
jurisdiction, is tied to the type of provider, or
other type of entity. Specifically, under the
original HIPAA statute, we have jurisdiction over
covered entities; three types of covered entities:
health care providers although not all health care providers, rather, only those that do electronic transactions such as electronic billing; health plans generally; and also health care clearinghouses, which I'll just say does not really relate to this discussion so I won't go into that in any great detail.

So, we also though under the HITECH Act now have direct liability, direct jurisdiction, over business associates which you can almost think of as an extension of covered entities in the sense that there cannot be a business associate without there being some covered entity that the business associate is acting on behalf of. I don't mean to suggest that it's always more of a master-servant relationship. I mean, often times there might be only one health information exchange for example and they may be a business associate even though they have all the cards so to speak, but the treatment is still that they are acting on behalf of covered entities in this context.
So the reason we're here today is to talk about PHRs. So are PHRs covered by HIPAA? The answer is sometimes, which I know that provides a clear, concise answer to everyone. So PHRs are covered by HIPAA when they're furnished directly by a covered entity and we saw an example of that with Kaiser, and also when they are provided on behalf of a covered entity by a third party. So that's really what you're looking at is the PHR provided on behalf of the covered entity which can be a very fact-specific test. It's not always easy to determine that. Interoperability for example, the fact that the provider systems may be connected to and able to exchange data with a PHR, that does not necessarily mean that the PHR vendor is acting on behalf of the covered entity even if they market it as such, even if there's an exclusive relationship, that does not necessarily mean that the PHR vendor is acting on behalf of the covered entity. Rather, we really look towards whether the PHR vendor is specifically providing a service to the covered entity for its
population. Often times this would take the form of some sort of an agreement, it doesn't have to be in writing, but a good factor to look at is if a PHR vendor refused to provide, for example, a PHR to one of the covered entities' patients or enrollees, are they in violation of some sort of agreement? Is there some sort reason that they can't chose not to? That's one helpful test. Certainly if money is changing hands, that can also be an important factor for looking at things.

PHR vendors can be business associates in some lines of business and not others so you could have a company that has a direct-to-consumer PHR model, but also has contracted with a number of covered entities to specifically provide PHRs to their population. In that case they may be covered by HIPAA with respect to the covered-entity population, but not covered by HIPAA for their direct-to-consumer population. So it's not as simple as saying whether a PHR vendor is necessarily covered by HIPAA.

Under HIPAA our rules include the
Privacy, the Security and breach notification rules. I'll save those details for a little bit later in the discussion. Our enforcement mechanism is that we do have civil monetary penalties that can be imposed for violations that used to be limited strictly to the covered entities themselves and used to be capped at $100 per violation, which may sound small but continuing violations could be up to $25,000 per calendar year and often times if you violate one provision it's often times likely that you're violating a number of provision so that that could add up under the old system, but post-HITECH the penalties have gone up significantly to a minimum rather than maximum of $100 and often times $50,000 or more per violation and then up to $1.5 million per continuing violation per a particular provision. So once again if you are violating 10 different HIPAA provisions, that could be more like $15 million per year liability so that the stakes have gone up pretty significantly here. With that I'll turn it back to Leslie.
DR. FRANCIS: Loretta, please tell us about the Federal Trade Commission.

MS. GARRISON: Thank you very much, Leslie, and thank you to OCR and ONC for hosting this important event today. First I have to give the obligatory disclaimer. I'm here speaking only on behalf of myself and not officially for the Commission or any individual Commissioner.

As Leslie said, I'm with the Division of Privacy and Identity Protection at the Federal Trade Commission. We are part of the Bureau of Consumer Protection so that as an independent agency roughly half of our mission is consumer protection and the other half very roughly shares antitrust review jurisdiction with the Department of Justice.

In our division, we enforce a number of laws relating to privacy and security such as the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act, and for those of you who receive your financial privacy notices from your banks, our securities firms and so forth, these
are notices that are mandated under the Gramm-Leach-Bliley Act. We also enforce Section 5 of the Federal Trade Commission Act and this is very broadly for the agency, it applies to unfair or deceptive acts or practices in or affecting commerce. So, in our area we use both of those prongs, the unfairness prong and the deceptive acts or misrepresentations prong in both of our privacy and data security cases. In the deceptive prong it means misrepresentations for consumers that are material so if you have a statement in your privacy policy or anywhere else that you make to consumers, that is a promise and it's material to the consumers in terms of the way they would make a decision, and that is wrong, it is incorrect in the sense of the way your practices are carried out, that is deceptive and it is a violation of the FTC Act. On the unfairness, if your act causes or is likely to cause substantial consumer injury which is not reasonably avoidable by consumers themselves and which is not outweighed by countervailing benefits to consumers
or to competition.

Now we also have in companion with our FTC Act, Section 5 authority on the data-security side, the Gramm-Leach-Bliley Safeguards Rule. This rule has the standard that is reasonable and appropriate safeguards to protect sensitive information. It is a scalable and flexible standard, and our Section 5 cases and our Safeguard cases, we generally track along the same lines so that our standard in security is reasonable and appropriate for the circumstances and that will depend on the size of the entity and the sensitivity of the information.

In our data security cases, our approach is that we are not complaint driven. We investigate when we learn about privacy or security issues, and I have to thank Joanne because when California announced its or implemented its Data Breach Notification Law, we had been looking before that for potential problems, but once the Data Breach Notification Law came out which clearly made public what had
likely been occurring before and unknown to the public, then our caseload or potential caseload jumped exponentially. Our cases typically involve companies that fail in very fundamental ways. They have either no or scant policies and procedures. There is no training. There is failure to address multiple attack vectors. And there are missed opportunities to prevent, detect or respond to intrusions. So we have now about 30 cases that we have brought to date, data security cases. They are all available on our website. Our respondents are varied. We've brought actions or have settled and brought under order a credit card processor, a security software vendor, mortgage brokers and lenders, data brokers such as Choice Point and Lexis/Nexis, a drug manufacturer, and a pharmacy chain and PBM, CVS Caremark, as well as most recently Rite-Aid Pharmacy and a number of retail merchants such as BJ's Wholesale Club and TJX and others. The types of sensitive information that we found about consumers and employees are financial information, such as
credit card and bank account information,
employment information and records, health
information including prescription information,
Social Security numbers, driver's license numbers,
and date of birth. The concern here is that this
information is very rich information for identity
theft, and so that if you have very sensitive
information of this type, you need to take steps
to secure the information. But the types of
security problems that we've seen run from
improper disposal of paper documents to electronic
security failures, such as poor wireless security.

Generally our cases stem from several
general principles. If you make a claim about
data security, be sure it's accurate. You should
protect against common technology threats. You
need to know with whom you're sharing sensitive
personal information. You shouldn't retain
sensitive information any longer than you have a
business need for it. And you should dispose of
sensitive information carefully. I just want to
highlight a couple of emerging issues which are
important and play a role in the health area. Peer to peer: we announced early this year an investigation where we had sent letters to about 100 companies that ranged from very small to major corporations that involved loss of or leakage of very sensitive information, including medical information on peer-to-peer networks because companies had allowed, or in some way peer-to-peer software applications were found on computers at the work place, and so information was leaked to these networks. When they are leaked in that manner then they're accessible to anybody who is on the network and it's very difficult if not impossible to retrieve it and to get rid of it.

Photocopiers are another issue. People don't realize that now when you do Xeroxing, those photocopiers have hard drives in them and they save and store all of that sensitive information, including just plain recipes or travel information that you may be copying so that you need to take steps to make sure that you either override those hard drives or contractually retain them and
I wanted to thank Colin for mentioning our FTC report that just came out. I have a copy here. It is available online. But some of the issues that we discuss in this report are very pertinent to the discussions we've had here. For example, online tracking or online behavioral advertising. Among our discussions in this report we've talked about a potential of a do-not-track proposal, in other words, to give some consumers not only awareness but control over what may be happening to their information. In addition, our view on sensitive information is that this includes information about children, financial and medical information and geolocation data, all very critical pieces of information that are at play in the PHRs and involve often medical data.

Health websites. We've seen that there is a proliferation of these kinds of websites, which also include social networking websites -- we've heard about some of this today. All of this as we discussed earlier, falls completely outside
of HIPAA. It means that are no baseline ground rules in terms of how this information is managed, collected, shared or disposed of and the only thing behind it is our Section 5 authority when we find unfair or deceptive acts or practices and we can bring an action against a company. We've seen as there are many different models for these kinds of PHRs and these other emerging health websites or social networking sites, there are as many different models as there are people in this room and they all have very different practices. And so one of the things that we've tried to lay out in our report is that we need to have some baseline standards of behavior by companies. We heard today from Colin and also from Microsoft about the fact that they appreciated the standards or principles that we laid out here and that they already follow them and that's wonderful. But many companies are under the radar. They are collecting this information and in fact they are not following standards that are the same as we've heard this morning. So with that I'll close.
DR. FRANCIS: California has a history of going further and perhaps covering some of the companies that are under or over the radar so I'm going to ask Joanne to talk about what California is doing.

MS. MCNABB: Thank you, Leslie. Thank you for inviting me here, whoever invited me here. It's been a very informative day so far. Just briefly for those of you who are not aware of the California Office of Privacy Protection, we are not a regulatory body. I would say I'm not a regulator, I'm a cajoler. We have a consumer privacy advocacy and education mission. In addition to educating and assisting consumers or individuals in exercising or asserting privacy rights, we also by statute make best practice recommendations to organizations. I was really struck by some things that Matt said about the focus in organizations needing to be on -- being trustworthy and talking about the ethical thing to do. That's sort of the approach that we take when we are being asked for advice from businesses and
organizations, talking about what is the privacy

protective ethical thing to do in that situation

which certainly would not be against the law.

I want to tell you a little bit the law

that Leslie alluded to but only a little bit

because I think we're going to get into it in more
detail later, as well as a couple of other

California laws that apply to PHRs. We have a

pre-HIPAA version of medical privacy law, the

Confidentiality of Medical Information Act, that

was amended in 2008 with the intention of bringing

in personal health records. It brings them in to

its scope by asserting that they are deemed to be

providers for the purposes of the Confidentiality

of Medical Information Act. The definition of

what I would call a PHR operator is a business

organized for the purpose of maintaining medical

information in order to make it available to an

individual or to a provider of health care at the

request of the individual or a provider for

purposes of allowing the individual to manage his

or her information or for diagnosis and treatment
of the individual. Got that? So it would seem to encompass a fairly broad spectrum of the types of PHRs, it would seem.

So by deeming such a business to be a provider for the purposes of the CMIA, that means that those businesses are then subject to the limits on use and disclosure of patient information that are in the Act. Those limits are very similar to HIPAA's in most regards, generally okay for TPO, otherwise it takes consent with the logical exceptions, public health, et cetera. And requires -- it also applies to contractors, so it also applies to in many cases what would be called business associates.

There are a couple of other privacy statutes in California that would also apply to personal health record businesses. One is our General Breach Notice Law which I did not pass I will say. I was there but I don't make those laws. It's a very interesting law and I know that many, many people feel that started a trend that has gotten things very complicated, but I think
it's one of the more effective privacy laws on the books in that it deals with the consequences of bad practices rather than specifying practices. Originally when that law took effect in 2003, it was focused on identity theft and focused on financial information: Social Security numbers as a factor in financial information and others. Effective in 2008, it was amended in recognition of the growth of or growing awareness of medical identity theft, it was amended to bring in medical information and health insurance information very broadly defined, but the medical information term that would certainly bring in any information that would be on a personal health record.

One other statute -- there are more that apply to businesses in California -- but another one that I think is particularly relevant that would apply to a PHR business that is subject to California law is the Online Privacy Protection Act, the California, our COPPA, which applies to operators of commercial websites and requires them to post a privacy policy and then to abide by it.
It doesn't have many specific requirements about what must be in that policy, but one of the requirements that I think that's particularly interesting and relevant and potentially useful in the area of online personal health records is the requirement that the privacy policy disclose the categories of third parties with whom information collected from site visitors might be shared so that's not just users, but visitors. So as we go on to talk a little more about some of the issues that are hard to address such as behavioral tracking, I think this law might be germane.

DR. FRANCIS: Thank you. What I want to do quickly now is look at, we've heard a little bit about how security is protected under HIPAA and by the Federal Trade Commission and we just heard California on breach notification. Both OCR and the Federal Trade Commission have a role at the federal level with respect to breach notification. I'd like Adam to add anything he'd like to add about the HIPAA Security Rule and then comment briefly on how breach notification works.
with respect to OCR, what it covers and quickly
how it works, and then I'll ask Loretta to do the
same thing.

MR. GREENE: Certainly. So the HIPAA
Security Rule consists of over 50 standards and
implementation specifications which may seem
daunting, but in fact almost all of these I would
expect are standards or implementation
specifications that one would expect in any
reasonable security program. And one thing that
some covered entities may misguidedly do is look
at these implementation specs distinctly and try
to take more of a checklist approach of OK have I
done this one, have I done that one. And the
Security Rule while it does include these more
detailed requirements, the most important aspect
of it is that you should have a cohesive,
comprehensive security program in place. So that
starts with a risk-analysis under the Security
Rule looking at what electronic protected health
information you have, where you have it, the
criticality of the different pieces of PHI and
then recognizing the reasonably foreseeable threats and vulnerabilities to that information. Then once you've done a thorough risk-analysis you then have to create your own risk-management strategy, which -- what people's favorite part and what people's least favorite part of the Security Rule probably is -- is the flexible approach. We often times have people going thank you for appreciating that not all covered entities are equal, that the appropriate security program for your large integrated delivery system is not necessarily the same for your single practitioner. Just as often, if not more so, we have people coming to us saying, OK I've read your regulation, could you just tell me what I need to do? The answer is you need to do what's reasonable and appropriate for your practice, which is going to differ based on factors such as the size, resources and threats to your practice. So that's the approach that the Security Rule takes.

Then most recently under the HITECH Act we've added the HIPAA Breach Notification Rule,
which is very similar to the FTC's Breach Notification Rule that Loretta will address and involves notification to the individual when there's a breach, it involves notification to the Secretary of HHS, which may differ in that if it's a small breach of under 500 people involved that can be an annual notification, whereas if it's a large breach of over 500 people then you have to do it without unreasonable delay -- no later than 60 days. As I think everyone in this room knows, those large breaches get posted, amongst other things, on the HHS website in what is I know lovingly called the Wall of Shame on our website. And also in certain cases where there are 500 or more people in a particular state or jurisdiction there is also a notification requirement for local media so that individuals may learn that way.

The timeframe for breach notification is also something that is frequently misunderstood. You'll often times hear people saying under HIPAA you've got 60 days and that's not accurate. Your requirement is to notify the individual, and if
it's a large breach the Secretary, without
unreasonable delay and that may not be longer than
60 days. Without unreasonable delay means for
example, the information is pretty
straightforward, doesn't require a long
investigation, you've set a fax to the wrong
number for example, you know all the facts, then
notification may be the next day or even sooner,
it's that you can't sit on it for 60 days and
that's something that's been a frequent
misconception.

With respect to business associates,
there is a breach notification requirement on
business associates but it's for them to notify
the covered entity and that's also without
unreasonable delay and in the worst case no
greater than 60 days, so that the responsibility
generally falls to the covered entity to notify
the individuals and that's based on the assumption
that the covered entity is probably the one that
has the relationship with the individuals,
although we recognize that in certain
circumstances it may actually be the business
associate that has the relationship, where for
some other reason it may be appropriate to
delegate that responsibility to the business
associate although the liability still falls to
the covered entity in that case.

DR. FRANCIS: Loretta, do you want to
comment, and I know we have to move quickly, on
breach notification at the FTC?

MS. GARRISON: Sure, just very briefly
on the security standards that I had set out
before, unlike HIPAA, we do not have detailed
specifications, we don't endorse particular
technologies because we do not want a checklist
approach, and in fact sometimes the technology may
work and other times it may not, but certainly
technologies will change over time. Encryption is
certainly one. We've had companies that say they
encrypted but they used poor encryption or they
provided the key to decrypt which means of course
the information was accessible. So again the
standard is reasonable and appropriate under the
circumstances.

Very briefly on the PHR breach notification, that was a specific authority that was given to the FTC in the HITECH Act. It's only for PHRs, it's only data breach notification and it's very similar in terms of the reporting requirements to the HHS standard. The trigger for reporting is the acquisition of information without the authorization of the individual, and we have included in our rule a rebuttable presumption that unauthorized acquisition will presume to include the unauthorized access to unsecured personal health record identifiable health information unless the vendor of the personal health records, the PHR-related entity or third-party service provider that experienced the breach has reliable evidence showing that there has not been or could not reasonably have been unauthorized acquisition of such information. So we want to make sure that if somebody gets into a database and in fact they move around it and they see the data and then they leave, that in fact
that is a breach notification or it meets the breach notification requirement under our rule.

DR. FRANCIS: Thank you. We only have 5 minutes left for this very rich part of the panel, or maybe seven or something like that. I want to ask Joanne to comment on what you see as the ongoing role of the states in privacy protection.

Will that work as a question?

MS. MCNABB: Sure. I know that Lee mentioned earlier an advisory body at the state level that’s been making policy recommendations to our state Health and Human Services Secretary regarding privacy and security in HIE, so that’s sort of an example. And really the challenge on that board I think exemplifies the challenge of the states versus the federal government. The challenge on that board is to find a way to preserve or enable the greater protections of consumer privacy that exist in certain parts of the California state law while facilitating some of the desirable results of information sharing across state lines and it is not an easy thing to
do. It's the old laboratories of democracy point
-- the states have been the leaders of the federal
government in establishing privacy protections in
statute in the past 10 years or so and there is
certainly, in my opinion, a benefit to allowing
them to continue to do so. The role of a federal
law in consumer protection as establishing a floor
is a good one and allowing the states to be more
protective, to offer more protections, seems to be
a good idea, that the federal government can learn
from that. I notice that these new federal breach
requirements are built on the state laws and tweak
it a little, for example making it a little less
intense than the California law which provides
greater protection and requires more rapid notice
of individuals. Is this going to be the last
thing I get to say?

       DR. FRANCIS: No, not necessarily.

       MS. MCNABB: If you're not going to get
to the other questions, let me quickly answer the
other two questions. I want to give an example of
one of the greater protections offered in our
Confidentiality of Medical Information law and that is the definition of marketing that is prohibited without consent. It is a tighter definition than under HIPAA and applies to a greater body of marketing communications that are made for remuneration and that could be construed to cover, I assert, online behavioral advertising and marketing in many of its configurations on personal health records. And are you going to ask about mobile?

DR. FRANCIS: Go for mobile.

MS. MCNABB: Be careful. My Office did a consumer guide a year ago on personal health records which is available on our website at privacy.ca.gov and the staff person whose assignment it was to do the research for that came back after 3 weeks and said my advice is don't do it, don't do it. I said OK, now let's stop and think. There are some cases where this makes sense and it's out there, so let's give people some advice. So I'm kind of in the same place about using mobile devices to move your health
information around. I want to say don't do it, don't do it. So what we would say at this point is we aren't giving any advice on this yet, just be careful, go slow, convenience may not be the most important value in this arena.

DR. FRANCIS: Thank you. I want to ask Adam and Loretta to comment on one example where they have partnered with respect to privacy protection. Then if each of them has something that they want to be sure that we didn't get to ask that's on the table, I think I have enough time.

MS. GARRISON: Certainly. The FTC and OCR did two joint investigations on CVS Caremark and Rite-Aid Corporation, which was most recently announced. In both of those cases the facts grew out of an investigative reporter working in Indianapolis who discovered that when he went to the dumpsters behind a number of pharmacies in the Indianapolis area, he found bags full of intact non-electronic, that is, pill bottles or other paper, with personal health information in it that
was simply available, publicly accessible, from these dumpsters. He collected these bags and he did a report on it. He then went to 10 cities around the country and found similar problems so that this is clearly widespread. We worked together, we thought that the synergies between our two agencies in terms of our authorities and our approaches would be beneficial to bringing the two companies in question under consent orders. Now our orders are different but they're complementary. The HHS order, as Adam said OCR has civil penalty authority and so that they were able to use that authority in both cases and get monetary funds.

Their order covers the disposal of PHI by the pharmacy for a period of -- it will be monitored for three years. They have to do independent outside audits of their practices on disposal of the paper in the pharmacy. Our order is much broader. We do what's called fencing-in relief so that we cover all information whether it's in paper form or electronic in our orders.
In this case we also covered not only the patients in the pharmacy but customers at the front of the store who went there to get prescriptions as well as employees and we said all of their information needed to have the same protections.

The order also covered not just the pharmacy but the PBM so that's why we brought Caremark into our order. Our orders are for 20 years. We require among other things an independent third-party assessment of the entire security practices of the company for every other year for the 20-year period. Are we going to have extra time here?

DR. FRANCIS: The three clocks on the wall are different. Adam, I'm going to ask you to comment briefly on examples, and that clock is the best one. So I'm going to ask you to comment briefly on the examples and then I'll ask each one of you for a parting shot. How's that?

MR. GREENE: Certainly. Well I'll just say that the experience – I actually before coming to OCR was over at the Office of General Counsel
and I was able to work with Loretta on these cases, and it just goes to show sometimes people are asking the wrong question when they say which agency should have authority over PHRs? It doesn't necessarily have to be one. Agencies can work together and sometimes we had a very complementary approach with respect to our different enforcement mechanisms so it was very helpful there and I think we're going to see this more also in the federal and state areas with the state attorneys general having authority under HIPAA, there's going to be more joint actions we would expect in that front. And so certainly agencies can work together and the results can be quite harmonious.

DR. FRANCIS: Thank you - last two sentences from each of you.

MS. GARRISON: Only two?

DR. FRANCIS: Or three.

MS. GARRISON: We heard a lot about trust today and about trustworthiness. Of course that is really dependent not on just an assumption
that you'll have trust, but it's on the way in
which you behave. There is a recent Ponemon study
that looks at -- it did interviews of hospital
senior managers and talked about their security in
their settings which were a number of hospitals,
but other kinds of medical facilities. Basically,
the report was pretty alarming because the overall
consensus was that security was not ranked very
highly, that in fact they've had a number of data
breaches, and in fact Ponemon was able to
extrapolate that the cost of these breaches not
just in terms of trust through what's called
churning -- that means in the retail sense that
you're losing people -- but also in terms of
dollars was running into the billions of dollars.
Here we're talking about PHRs saving money, but if
you're really going to save money you need to
build in at the very beginning your privacy and
your security because that is part of what makes
you have a trustworthy product.

Now a couple of things. What John Moore
said which was a little alarming was of the 20
PHRs he said that he had surveyed only 2 years ago, that most of them have disappeared. The question is what has happened to the data that they had? We had a case recently where we heard about a bankruptcy setting where there was a customer list of a magazine of young male homosexuals and that customer list was viewed as an asset, which the court was going to sell. Our Bureau Director David Vladeck sent a letter to the judge asking that it not be sold saying that it was contrary to the promises made by the company in its privacy policy, that the disclosure of that information to this other group would be very damaging to these people, and to the judge's credit he in fact ordered that this be destroyed. I agree with Joanne also that the move to mobile is one that you need to be very careful of. We've had a lot of problems with wireless technology which of course is being used increasingly in hospitals where that's been a very vulnerable point in terms of entry into a system and to get access to information. So you need to have
caution. Security by the way is not a checklist. It's an ongoing defense in-depth. You need to build redundant systems. You need to do risk assessments as an ongoing process to make sure that in fact you're meeting current vulnerabilities and threats.

DR. FRANCIS: Thank you. Adam?

MR. GREENE: I think one of the biggest challenges in this space with PHRs especially since they are by definition really the closest link to the consumer is protecting individual's privacy without necessarily making their privacy decisions for them. We have an evolving marketplace here and the potential to unfairly stifle innovations based on assumptions that may be false about what values people have with respect to privacy is a very tough area, so that's one, I think, of the biggest challenges that we have moving forward in regulating this area.

DR. FRANCIS: Joanne?

MS. MCNABB: I kind of blurted out my closing lines earlier. One last closing thing. I
think you heard a lot about the ignorance -- lack of information -- ignorance, that individuals, that we all have as individuals, about how our information flows and particularly in a medical context. I don't think that the takeaway for people in the business side of the medical industrial complex should be we have to do more patient education first, that in fact it's the trustworthy practices and secure systems that need to come first, that the burden can't all be shifted to the consumers.

DR. FRANCIS: Thank you all very much and let's have a round of applause for these folks. [Applause].

We're going to move to - well, we've already been partly on the question of what should be happening with respect to considering rules, standards and the like and we're going to move more directly to what should be. I'm going to ask these panelists to shift and we'll have a change in guard.

My last three panelists are, on my
right, Robert Hudock, who is Counsel at EpsteinBeckerGreen. On my immediate left is Frank Pasquale who is the Schering-Plough Professor in Health Care Regulation and Enforcement at Seton Hall Law School and a Visiting Fellow at Princeton University's Center for Information Technology Policy. And on my very far left is Nick Terry who is the Chester A. Myers Professor of Law at St. Louis School of University School of law. Both Frank and Nick are prolific writers in the area of health policy and health information technology and more specifically on personal health records.

I'm going to start this panel off by asking -- going this way -- alphabetically for each of the panelists in a couple of sentences, maybe a paragraph but no more, to give us an overview of what each sees as the core regulatory choices to address when we think about PHRs that are not covered by HIPAA.

MR. HUDOCK: Thank you. We have a range of options available to us as we see the HIPAA Security Rules and regulations in the Ponemon
study that was spoken of by the colleague from the FTC where we're looking at a billion-or-so breaches. One of the most useful forms of documentation and support to people in the private industry with respect to HIPAA privacy and security was the NIST 800-66 publication. I see something similar to that being very useful for the public health record situation where an educated body can provide meaningful guidance about what a PHR is and what sort of security controls are appropriate.

DR. FRANCIS: Thank you. Frank?

MR. PASQUALE: Thank you. I think just to run through some of the core issues that I think are both going on right now and emerging, I think one clear one that we will get into later on the panel is what levels of security are necessary for these types of entities, especially the FTC regulated entities. The second is the nature of consent, whether it's general and how far general consent can go and where specific consent needs to be used. A third is about data integrity and
disputes over that. The Boston Globe had a very interesting article recently about a dispute by someone who found that lots of records loaded into his personal health record he felt were inaccurate but that he felt that he couldn't actually get at them and try to change them. There might be best practices from the Fair Credit Reporting Act in terms of how to access and ensure that sort of integrity. A fourth issue is banned uses. Are there any sort of uses or compelled disclosures that we need to ban or just stop at the outset in order to encourage people to really want to become part of personal health record systems? My final point I guess would just be that what are consumer expectations and how should those play into that? I think that's been a big divide today between those who really emphasize consumer expectations and others who stated that given how fast the technology is moving maybe we should try to get the regulation ahead of expectations as opposed to sort of letting it continue to erode them.

DR. FRANCIS: Thank you. Nick?
MR. TERRY: Thank you, and thanks for the invite and to you guys for hanging around and the three people who are on the web thing who logged in thinking it was World of Warcraft, welcome.

So first, terminology. Security regulates unconsented-to access to data whether outside hackers or insiders without authorization. That has to be distinguished from privacy regulation, which regulates data collection, its acquisition and in some countries with better privacy protection its processing. Third, confidentiality, which is all that HIPAA does, which is to regulate the disclosure or dissemination of data. That's my first problem, making sure we have the terminology right.

The second concern I have is definitional. What is a PHR? Specifically, are PHR privacy, security, confidentiality issues truly distinct on one hand from the HIPAA-regulated EHR and on the other hand do they pose any different problems from the average
website that allows medical data to be scraped off it, so I have a real problem with sort of trying to come to terms with the word PHR. Then the third major area that interests me when we look at the regulatory models; firstly, the problem of the regulatory indeterminacy as medical data gets pulled and pushed out of EHRs, back into PHRs, and then back again as to which particular regulatory regime applies at any one point and sometimes more than one will apply. Then finally, before Leslie has a stroke, I'd like to get back to some basic discussion of some basic privacy protective principles. I'd like to talk about proportionality later today and move away from what I think are defective models that we put in instead of true privacy, things like consent privacy policies. I have a long list.

DR. FRANCIS: Thank you, and I hope we get to at least some of that list. For starters, I'd like each of you to think about security with us for a minute and pick one security issue that you think ought to be on the table, thought about
as ongoing choices get made and I'll continue to
go right to left.

MR. HUDOCK: Security in the traditional
sense means confidentiality, integrity and
availability, and I believe integrity is the
biggest problem and that we really haven't been
focusing on the implications of incorrect data,
data quality. It's not only having the patient
have the right to correct the information, it's
about having maybe a PHR where the patient can
manipulate the data. Then we also see where
depending on the source of the PHR, the physician
doubts it more or less, really that's all about
integrity of the PHR. Can I trust that other
physician who's across the country on the data
that they inputted? We haven't seen much guidance
on how to know whether that medical record or that
PHR is something that I can rely on.

DR. FRANCIS: Thank you. We've talked
about data integrity. The next security issue?

MR. PASQUALE: I wanted to pick up on a
contribution that I think both the Markle
Foundation and the Center for Democracy and Technology have made in this debate and other debates which is on Immutable Data Trails and we've heard a little bit about that earlier this afternoon, but I think that one key to ensuring data integrity is being aware of the versioning of the record of what got input where, when, at what point, watermarking interventions or any other efforts. I think that type of technology, sort of write once, read many type of drives; things used even by Wikipedia in order to keep versions of things correct. There are lots of very interesting technology out there and I think that trying to integrate those types of immutable audit trails, that should be a baseline minimum standard. The other ideas that I think are out there that we can get into more detail later on are learning from the use of research data. There are lots of debates in pharmacogenomics regulation going on right now about the ongoing convergence of people's data, people being seen as patients who are to be treated and then as research
subjects. I think as we see this sort of proliferation of uses for the data, that's going to be very important to all of these security issues, I mean there is lots of stuff out there in the Common Rule and other sort of areas impinging on research that talk about delinking, de-identifying, particularly identifying, reidentifying of data, and I think learning from those areas would be very key here.

DR. FRANCIS: Thank you. Nick?

MR. TERRY: Again securing what?

Securing a website that people are posting on? Do we mean securing the LBS, location-based services, of people's mobile devices? Or the one I'm going to pick on which is securing the data stream, the coffee shop problem, the WiFi problem. I think it is unconscionable that any website whether it's a PHR site or not that takes, that requires individual identifiers to logon such as a user name or password does not use a secure layer and the FTC should whack them for it.

DR. FRANCIS: Let me ask just a little
follow-up on SmartPhones and I'll tuck that in here about security issues. Are there separate security issues with SmartPhones that you think, Robert, we should be reminded of here?

MR. HUDOCK: Well, I see SmartPhones as being more secure than your typical computer for a couple of different reasons. For example, most of you may or may not realize that SSL is really broken and that's the encryption protocol that we use for communicating sensitive information over the Internet. Now, cell phone communications follow an entirely different communications protocol so when I'm sending something over the cell phone network itself, I'm a little bit more comfortable than I am when I'm sending it over an Internet browser.

Now with that distinction I'll go on to say that I think that the right strategy right now for mobile telephones and iPads and things like that is to let industry evolve because I think that what we're going to see are consumers going to become interested in PHRs because of their
mobile device. But we can't really perceive
exactly how that mobile device will be used right
now. But a couple of positive things are
happening. For example, Apple released a version
of the new IOS for the iPad that has a FIPS-140-2
encryption built into it. That's a good thing.
It's nice to see that the technology vendors are
moving in that way. So I'm hesitant to put
restrictions on a technology where we don't
exactly understand how it's going to be used and I
think that moreover it's going to hurt adoption of
PHRs which in the end I think are going to be what
our EHRs will be because this PHR/EHR thing is so
nebulous that who knows what's what. I think
we'll end up with something like a PHR that will
be driven by consumer demand and it will come from
the mobile telephone industry and SmartPhones.

DR. FRANCIS: This sounds rather
different from taking HIPAA and expanding it out.
One of the questions on the table is whether a
possible strategy here would be to take the HIPAA
Security Rule, after all people are accustomed to
HIPAA in the health care setting and some of this data come out of the health care setting. So I'd like to ask any of the rest of you or Robert to comment on, the first question I'm going to follow-up on here is, whether it makes sense at all or any comments people have on expanding the HIPAA Security Rule to other PHRs that are currently not covered entities? The other question we're going to look at is whether the Federal Trade Commission, what authority people think that -- or would it take statutory change to think that certain kinds of security practices or poor security practices are unfair trade practices. First let me go to HIPAA and any comments on the pros and cons further on expanding the HIPAA Security Rule.

MR. TERRY: I think HIPAA -- unless you tear it up and start again and do something more like the California model which impresses me -- I think HIPAA has probably been extended through HITECH to the BAs as far as we probably are going to be able to do it. There is also a sense I
think that one has that privacy, confidentiality, security at least traditionally, historically, have been addressed contextually. We look at these vertical segments or domains or subdomains and we come up with privacy, confidentiality, security models that we think are best attuned to those. A good example of that is, and I think I ripped this off from Helen Nissenbaum's book "Privacy in Context," imagine if every single move you made was being written down or even filmed, that everything you said or did was being documented, that every mood swing, every piece of information over 24 hours was being documented. You'd go - oh that is just Orwellian. In a hospital that's what we could call good care, so that I think context is really important.

The other thing is that legal norms by themselves don't always win, and so it's important to tune your legal norms to existing social or ethical or professional norms. The hospital/physician environment has those set up so that one of the challenges for the regulator is to
find legal rules that map to those and there is mutual reinforcement. I don't really see any of those existing rules operating for the untethered as I call it, the pure PHR, and therefore I'm not sure there's much point in trying to - in wasting energy in trying to extend HIPAA to those types of PHRs.

DR. FRANCIS: So that would start us with the Federal Trade Commission. The question was, and I'll ask Frank to address this, whether we need more than the current unfair or deceptive Section 5 authority to address security if it were to happen through the FTC rather than through HIPAA.

MR. PASQUALE: Thanks. I think that we've seen some really impressive initiatives out of both ONC and FTC and the FTC does have a lot of powers and it's a broad statute, the Section 5 of the FTC Act, so you've got a lot of adjudicative powers there and a lot of, I think, room for say even rulemaking to really delineate what best practices would be and what these entities ought
to be doing. I think the problem comes with what
happens when you start seeing sites pop up, and I
think this was mentioned briefly by Loretta
Garrison, that may say we offer no guarantees,
what if you get sites that just say listen, you
put your stuff up here, we really don't promise
anything. I think that is a possibility and even
when you talk about changes of attitudes toward
privacy, you have to start worrying about that,
and you have that description on The Wall Street
Journal's "What They Know" series, an incredible
series at wsj.com/wtk, "What They Know." They've
done a great job of showing how data can sort of
be unleashed.

And I just want to give, in this sort of
privacy in context, I want to give a flip side of
Nick's hospital example. There was a pretty
astonishing article in Business Week that was out
there that talked about -- a couple of years ago
by Chad Terhune -- the use by individual insurers
of pharmacy records and medical credit scores that
were sort of being developed in other ways and
these pharmacy records were being used by
ing individual insurers to figure out if they wanted
to insure people or not. So my worry is all
right, I may think that by and large the personal
health record vendors are quite fine, but where I
get worried about is when you possibly have data
that's gone legitimately from the personal health
record vendor to some other entity that it's been
authorized to share that data with and then maybe
it gets beyond there; there's a lot of literature
out there on privacy now on so-called data
laundering or fourth parties. Lots of rules that
apply to third parties like telecommunication
providers may not apply to fourth parties like
data brokers. My ultimate concern, I guess, is
that this sort of security may involve
watermarking of individual data so we know where
it is, we know who has it and ultimately that's
going to address the concerns that I think a lot
of consumers have about possibly having their data
being used adversely to them and be things like
employer scoring, insurer scoring. And just to
give one final example of those sort of brave new
world possibilities. Sharon Hoffman, who's a
really fantastic legal and technical expert in
this area, has brought up the possibility in a
recent article that employers could have access or
somehow have access to these types of records,
that they could develop scores on individuals on
whether they are likely to get sick and that's
very worrisome. I think that because there's the
possibility of that data going out unleashed, we
have to try to build into the technology and
regulation at the beginning of the creation of a
record ways of avoiding those very troubling
scenarios.

DR. FRANCIS: Let's turn specifically
now to privacy. I'd like to ask each of you to
pick one -- well I should call it given the way
the terms were set up at the beginning --
confidentiality -- one important issue with
respect to the sharing of information and consumer
knowledge or control so that would be
confidentiality in a technical sense that each of
the panelists would like to be sure that gets talked about. Nick, we'll start with you on the confidentiality front.

MR. TERRY: On the confidentiality/privacy front, I guess the piece that worries me the most at the moment is data scraping from websites. Generally again as Frank was talking about both The Wall Street Journal and the Times recently picked up on some fascinating stories -- PatientsLikeMe is just one of them -- and there's this new complaint that's just been filed by privacy advocates with the FTC with regard to some of these activities and I think that constellation of activities and the activities of data aggregators generally and what is happening with this data whether you track it or not are probably where I'd put my energies.

DR. FRANCIS: Could I ask you to elaborate a little bit for some of the uninitiated to describe exactly what you mean by data scraping?

MR. TERRY: As I understand it, it is
with various levels of consent or conspiring by
those associated with the site, sometimes existing
members, sometimes simply data robots that are
being sent in, that are literally scraping off the
data that people are putting on these websites
with regard to their medical diagnoses, with
regard perhaps to pharmaceuticals that they have
been prescribed and various other pieces of
information, some of which is identifiable
immediately because they may have their own names,
others as I believe was the case with
PatientsLikeMe may not have been directly
identifiable because people posted with
pseudonyms, but because there was linkage or
possible linkage that could be made to social
networking sites, their actual identities could be
discovered. Those are collected along with whole
bunches of other information, such as data from
prescribers and from pharmacies, and are
aggregated in a multibillion-dollar industry and
sold back to health care providers and
pharmaceutical companies, as I understand it.
DR. FRANCIS: Thank you. Frank, you want to comment on a confidentiality issue?

MR. PASQUALE: Nick has addressed many of my deepest concerns here I think in talking about the scraping issue. I do think that the one corrective here that I think could help a lot would be -- I don't necessarily worry all that much, let's see if I remember PatientsLikeMe if someone has copied all the data and they have that data in some vault somewhere that's associated with that user name, I mean I do start to worry. But where I really get worried is when that data becomes actionable and when it gets combined say with other data and somehow gets used to create a profile of me and I think that's something that I was so happy to see the FTC's action on behavioral advertising now because I think what it's doing is the agency is trying to make people more aware that we all have a digital self that's out there, the sort of digital doppelganger that is associating various characteristics of past behavior or past identity or past associations
with us. I think to the extent that one way to
make people feel more comfortable about the
inevitable losses of privacy or inevitable sorts
of breaches that may occur is that when this sort
of digital self is created by these new profiling
tentities be they online behavioral advertisers or
other profilers that we have some opportunity to
understand what data they're using, how they're
using it -- be more open about it. My nightmare
scenario is that you have a scenario where
reputation scores like credit scores get created
that are black boxes. The worry about the Fair
Credit Reporting Act is yeah, there are lots of
abilities to actually change your report, but how
much does that really mean to the average person
if the only thing that matters is scoring and you
don't know how the score is created? So I think
that's a very important aspect of this is that we
have to be aware of the frontiers of reputation
creation and profiling based on data that may get
out there.

DR. FRANCIS: Robert?
MR. HUDOCK: OK. I've been thinking about this as you've been coming down to me. There's a legal problem that I see with privacy and there's a technical problem that I think is a bigger issue. My biggest legal concern with privacy is that we have 50 different states with 50 different rules on how to get consent to share information and what a PHR is, what information should be shared and in what context. But ultimately the biggest privacy issue I see is sort of a consumer interface. They get this information on the computer and we've mentioned something about peer-to-peer file sharing before and a lot of consumers have that on their machines. So they download some of their medical information to their personal computer and then their child installs some peer-to-peer file sharing software on there, which is automatically configured to share all sorts of things from your computer, so all your tax records or whatever get popped up there. My biggest concern right now is for the average person being able to protect his
or her family as they get this information and I don't think that that can happen by adding a new piece of software to their computer. I think that has to happen where the internet hits the house. So my biggest concern is I think that whatever we wrap around PHRs for security, wherever we wrap around EHRs, whatever we wrap around other sensitive information is for naught because other stuff that's unrelated will end up leaking the information and it will happen from the consumer's house and it will be the consumer's fault because they won't know what to do.

DR. FRANCIS: So is it hopeless to think that -- we've heard a fair amount today about how consumers don't understand what it is to have a privacy policy and so do things that they didn't mean to do or don't read things because they think they didn't need to read them because they thought they protected them when in fact they didn't. What I want to do is ask each of you to comment moving further on this question of do you see any hope for the role of the consumer and consumer
348
1

choice in this or do you think that those

2

strategies are going to need to be strategies that

3

say that there are just certain things that

4

shouldn't happen or is there another way around

5

this that may be at the actual point of sharing no

6

matter how it happens, that at that point you have

7

just-in-time consumer consent?

8

strategy?

9

Nick and back to Robert.

10

Is that a

I'll start with Frank and then go to

MR. PASQUALE:

Sure. There are a lot of

11

challenges here and I think that there is one

12

thing that I'm glad to see some earlier panelists

13

talk about was the information overload problem,

14

that even if the privacy policy could be brought

15

down from 25 to 12 pages to 10 pages, still there

16

has got to be prioritization in terms of what are

17

the most important things in it and what are

18

really critical to people and I think that's where

19

these surveys that we had earlier are really

20

valuable because they can point to us what do

21

people really value.

22

On a more technological level, there are


some ideas out there about the segmentation of

data in the record so that if you really want to

have a segmented record such that part of the

record never gets shared except with your explicit

personal permission for every particular sharing

possibility, you may want to just pre-commit

yourself to that and Viktor Mayer-Schönberger's

book "Delete" talks a lot about the sort of

technical protocols that might be involved in

that, the same with Jonathan Zittrain's book "The

Future of the Internet and How to Stop it" -- he

worries about the future of the Internet -- and he

talks about having a green box and a red box on

your computer, a green zone and a red zone, and

the red zone is where you connect with everybody

but you don't keep really safe things there

because you know it's going to be exposed to the

public internet versus the green part that's more

secure.

Finally, the final technological thought

that I think is somewhat helpful here is what

Jerry Kang's group at UCLA has been dealing with
sensor networks and has come out with the idea of a personal data vault. We heard earlier about sensor networks being used in health care and I think that as that type of ubiquitous computing ends up feeding more and more information about us or if we sign up for that, we need to have that option because my final rationale for this would be opting-in to things like quantifying yourself or these other things, it may seem like an odd habit of nerds right now, but I promise that as wellness programs and other sorts of benefits become more popular it's not going to be easy to avoid them. People are going to wonder why aren't you part of the quantified-self movement? What are you trying to hide? Are you trying to hide your cholesterol level from us? I think that even though they seem that they are the vanguard now, this privacy phenomenon called unraveling can very quickly lead a tipping point where everyone feels not just that it's helpful but that they need to be part of these things.

DR. FRANCIS: Thanks. Nick?
MR. TERRY: It's a huge surprise that I'm kind of skeptical with regard to current privacy policies and so on. I think privacy policies are like warranties that we saw in the 1960s, that there are actually lists of things they're taking away from us rather than lists of things they're going to give us. I think that what we see today is still the discredited notice and choice model of privacy, that is, you've been given notice and that's the health privacy we're taking away from you and therefore you've been deemed to have been given a choice. So long as vendors and suppliers of these websites and PHRs, untethered non-HIPAA PHRs, as long as the vendors control the choice architecture then I don't think we're going to have major improvement.

The other thing I think that the current phrase that everyone wants to use is trust. Trust is really big at the moment. We have trust. Our PHRs have trust. Everyone wants to talk about trust, but I don't know what they mean by trust when they talk about it. I think the only people
that most of these companies that know the meaning of trust are their marketing departments and I think it's a piece of branding. I think trust has various meanings. I think the meaning of trust changes as to context. And also I think trust changes as it scales or that what you're doing scales, so I don't think anyone should be allowed to use the word trust in this without defining it and if they don't define it then we should shout at them that's not trust, that's as Steven Colbert would say trustiness.

DR. FRANCIS: Robert?

MR. HUDOCK: Could you specify the question a little bit more?

DR. FRANCIS: What I want specifically is a comment on whether more information to consumers about what their kids might do with file sharing and what might happen if their kids install a file-sharing program whether that's at all likely to be helpful or whether what we ought to do is have ways that information from PHRs just can't get on computers that have file sharing. So
the question is whether it's consumer consent and
more information to consumers that's a strategy or
whether you see that as hopeless.

MR. HUDOCK: I guess I see it as a
little bit of hopeless and the reason why is the
Internet really wasn't designed for the secure
environment that we want to put it into right now.
The basic protocols were designed back in the
1970s where just only a few universities connected
up. I think we have to reengineer how our
Internet works in order to be able to build in
security that actually works because right now, I
just don't know -- we can't rely on the methods
that are being provided to us to secure the
information over the Internet as being 100-percent
secure. We can't do layered consent models where
you have different levels of access based on
digital keys and things like that. I think this
technology needs to be developed and it needs to
be pushed out and it will probably take a long
time because we had a problem with the DNS and it
took forever to get a secured DNS system out, so
invest in technology to get a better Internet.

DR. FRANCIS: Thanks. I have a quick question for Frank and Nick about models from elsewhere. We've been mostly talking about what's going on within the U.S. and there are some approaches elsewhere and I know Nick knows something about approaches elsewhere and I think, Frank, you know something about that.

MR. TERRY: You said this would be a fine 10-day conference. The two pieces that I think are useful. One, is what is -- the core of the E.U.

Directive -- is privacy and confidentiality in that it seeks to regulate not only the dissemination of data, which is primarily what HIPAA regulates, but also the collection of data and it puts a proportionality rule with regard to both of those. It then also layers on top of that a far stricter rule when you get to things like medical data as opposed to other types of data. I think that's the big lesson from there without getting too technical.
The other lesson I think that is worth looking at, although there is some flux at the moment as they reorganize, is the Australian model in two senses. First, they have an identified privacy curator, a privacy commissioner, someone who has an independent role and is somewhat depoliticized and has a role in working with both industry and consumer organizations to improve privacy. Those kinds of privacy commissioner institutions are very good at putting out policies and practices and fine-tuning and working with industry and consumers and I think there is some interesting stuff that could be done there, again without wanting to get too detailed.

DR. FRANCIS: Thanks. Frank?

MR. PASQUALE: I'll quickly add onto that that part of the E.U. Convention on Data Protection Regarding Individuals says that personal data including health data can't be processed automatically unless there are appropriate safeguards and I think that sort of model of trying to have some level of reporting
and explanation of what's going on with the processing before it happens might be something that we should look into.

I think also that the French agency CNIL has a great website that describes a lot of what they do and as I was looking at the Center for Democracy and Technology's comments on today's events, one of the things they mentioned was people being able to demand or to ask from personal health record providers or those that have their data who it was shared with, to be able to get that type of data. One of the things that the CNIL has been at the head of the curve on that is implementing those types of rights of consumers to understand where their data has been and that type of auditing capability, so that I think there's a lot for the U.S. to learn from the CNIL.

DR. FRANCIS: Robert has a comment on that and then I'm going to ask each of the panelists to give us last thoughts.

MR. HUDOCK: Actually, this comment supports some of the material that we've been
presenting and that is the Ponemon study that
actually studied the United States and the cost of
security breaches per record. They actually
studied Australia and the E.U., and the cost of
security breaches per record in Australia and the
E.U. is significantly less than what it is in the
United States so that that may be an indication of
what they're doing is working.

DR. FRANCIS: Each of the panelists and
since you have the mic, Robert, I'll start with
you. What do you regard as important last
thoughts as we go forward into this brave new
world where are sort of already somewhere in the
middle of?

MR. HUDOCK: I'm a little nervous about,
I'll give you just my 10 cents of advice here and
it really is less about PHRs and more about kids.
I've got three kids and they are little ones, and
I worry about them getting on the Internet so that
my little bit of advice is think about your
security because I think that that's where it's
going to have to happen, whether it's a PHR,
whether it's a Facebook or whatever.

DR. FRANCIS: Thank you. Frank and then

Nick.

MR. PASQUALE: I think my very specific
points might be that I do think that there is an
important role for states here where a state like
California, just as led with emission standards,
can lead in other ways and be sort of a lab for
innovation and I think if Google Health and
amazing companies in the Silicon Valley can
survive the California regulatory regime that
others can as well.

I think consumers' private rights of
action really should be looked at and that's a
really interesting way of diversifying authority
to make sure that things are happening correctly.
My final point, the broader point, would be that I
think there is no necessary tradeoff between
privacy, security and innovation if the privacy
and security are done right, and in fact, the
privacy and security goals and standards may be
the real foundation we need to see major
innovation here to really get widespread adoption
and diffusion of this innovation. So I would just
caution against the usual tradeoff frame of mind
there and really emphasize how these two things
can be reinforcing.

DR. FRANCIS: Thank you. Nick?

MR. TERRY: I've been talking about
proportionality and I don't know what that means
to you, but here are three things that I think --
three meanings that it has. You can only collect
data when it's necessary for the announced purpose
for which data is being collected. It's akin to
the minimum necessary rule but on steroids. You
can only use the data that you collect for the
purpose that you say that you're collecting it
for. Third, you can only use, store or process
that data for the time necessary to complete that
purpose and then you have to get rid of that data.
Anything outside of that is a disproportionate use
of someone's private data.

In the medical domain we failed I think
in HIPAA by trying to use a surrogate which was
TPO, treatment, payment and health care operations, for that proportionality. And Leslie and I have bored people with articles in which we say that a better approach would have been medical domain or circle of care or something like that and that's fine by me. Outside of the health care domain when we're looking at PHRs and unprotected websites and so on, I would actually take a far more radical approach to try and get to some proportionate use and I would use a property rule. I would say that the data cannot be sold or bartered if it is medical information data and I would put a prohibition on that. I would let it open for nonprofit uses and so on so our outcomes research folks and our effectiveness researchers and so on are still in that game. But I would simply prohibit a market in private medical information. I think that's consistent with what GINA is doing, the Genetic Information Nondiscrimination Act. I think it's consistent with these new New England Statues dealing with prescribing information. I think it's consistent
with HITECH's approach to EHR data. And I think an inalienability rule, a market inalienability rule as it is called would be a spectacular approach and a good way of achieving proportional use of data in this space.

DR. FRANCIS: Thank you. Thank you to everyone on this panel as well as on Panel 4-A. We need to now turn the microphones over to those who have been patiently waiting out there in cyberspace for their turn, so it's time for visitor input as well, for public comment. Thank you to Robert, Frank and Nick for wonderful presentations. [Applause].

MS. PRITTS: While we're setting up the phone, we're also going to be able to take some comments from people in the audience here. There's a microphone in the back so that if you have a comment, please go to the microphone in the back. We're asking people to limit yourselves to two minutes and I am going to be very strict about the two minutes. Anybody who has seen me in action before knows I mean it, so we'll wait until
we are set up here so that everybody can hear
before we start. If we could have our first
commenter from the in-person meeting, please.

DR. POTARAZU: I'm Dr. Sreedhar Potarazu, the CEO for VitalSpring. We are
currently launching in phase one, 15 regional hubs
of integrating every employer to every provider
and we're issuing the report by December 10 of
over 40 of the Fortune 100 companies on
integrating the work health record with the
electronic medical record into a personal health
record. The thing I didn't hear the entire day
today was a practical issue we're dealing with
right now on the integration of coverage data,
nothing to do with clinical data, but coverage
data -- basic financial information that consumers
want to put into a personal health record which is
not feasible in any PHR today. All of the data is
currently unstructured data. There is no means to
pull in structured data and we've spent a lot of
time in terms of talking about clinical
information, but the problem we have right now
with hundreds of employers and millions of people across the country are trying to put in basic coverage information. The new law around ARRA is focused on coverage and access and very little on care and the biggest problem we have right now is providing consumers transparency on cost and nothing to do with clinical care and we have no means of addressing that right now. So the report that comes out on the 10th is going to address the immediate challenges that these 50 companies across the country have.

MS. PRITTS: Thank you. Are we ready to take a call?

OPERATOR: The first question comes from the line of Lester Keeger. Your line is open.

MR. KEEGER: The panel was excellent. Robert talked about the cost of security. This could be taken care of with proper protocols right up front.

MS. PRITTS: Thank you.

MR. KEEGER: The next thing is that Frank talked about industry investment, the
upfront ID, and that means that the -- attached
two actions, properly taken care of can really
make a difference.

MS. PRITTS: We're getting an echo in
here - is that from the speaker? Can the speaker
please turn off the webcast?

MR. KEEGER: Yes. I apologize.

MS. PRITTS: Thank you.

MR. KEEVER: Let me say it again.

MS. PRITTS: We've heard it I think four
times. If you could move on to your next point
that would be appreciated.

MR. KEETER: Are you talking to me?

Sorry.

MS. PRITTS: Yes, sir.

MR. KEEGER: Frank talked about
safeguards before it happens. This is exactly
right. Robert talked about costs of security --
stopping fraud can be a big payoff and that's
exactly right.

Handling data with proper protocols up
front would take care of this. That means that if
you can have the proper ID attached to the specific person with RBAC, your controls attached to the action, that can make a big difference in cost and implementation of security and privacy.

MS. PRITTS: And by RBAC you mean role-based access?

MR. KEEVER: Yes, ma'am.

MS. PRITTS: Thank you very much for your comment. We are now going to take another comment from the room and then we'll take our next comment from the room. Sir?

MR. PHELAN: My name is John Phelan and I'm the CEO and founder of Zweena. It's been incredibly challenging to be in this room all day and not ask questions so that I think there is a missed learning opportunity, quite honestly. I'm not impressed with my government here today. I would much rather have an opportunity to ask organized questions during the panel because I think there is a communal learning here that happens from other people's questions, so that's just a general comment.
I have really two things very quickly. One is CCR/CCD standards. As we digitize discrete data, which my company does for consumers, we as the United States need to have one standard. I didn't hear anybody talk about that today and I know we're talking about privacy and security, but quite honestly, consumers want their information digitized. They're not going to wait for their doctors, they're not to wait for their hospitals, and that's what we're doing for consumers in 12 different states today.

The second issue really is around certification. We as a company that's pioneering a lot of this is having to really talk amongst ourselves and kind of prop ourselves up and be good corporate citizens and in many of the discussions that were talked about today on privacy and security, we're employing all of those, and in fact employing more than those. So we're hoping that somebody like ONC or some organization within the government is going to be certifying not only EHRs and EMRs but also PHRs
and we're looking forward to being part of that process.

MS. PRITTS: Thank you. Can we get back to the phone now?

MR. MALDONADO: Hello. Thank you to everyone for a very informative few hours. My question is about the apparent relative lack of concern concerning one form of government-sponsored PHI dissemination versus another. The one that I'm referring to is the NHIN Connect platform or model or recipe, and the NHIN Direct model. The NHIN Connect model is a model for sharing EHR information among provider institutions and is very well founded with a lot of projects rolling out. The NHIN Direct is a newer model that relies on email, fundamentally as the protocol, although there is another approach and seems a much more consumer-oriented, a la the PHR. I'm interested in your panel's comments on the relative strengths and weaknesses of those two dissemination models with respect to confidentiality.
MS. PRITTS: The conference today is centered on PHRs and we have no panel left to discuss these issues so we appreciate your comments and will take them under consideration. I'll now turn back to comments in the room, please.

MS. WALDO: Hello, I'm Ann Waldo. I'm a privacy attorney here in Washington and I'm representing Genetic Alliance today. Genetic Alliance is a nonprofit health advocacy organization that serves as a network of over 10,000 patient groups, and government institutions, and medical researchers and industry. We support a broad array of health care goals, improving patient access to care and above all accelerating breakthrough medicines and new tests and treatments. We are very much in favor of PHRs and we're delighted with the changes in the Stimulus Act that expand patients' rights to electronic copies of their records and getting them into their PHRs in a more seamless and efficient manner.
We do have one small concern that I wanted to lay out which has to with a small requirement in the HITECH NPRM, the proposed regulation, that came out this summer. The statute says that patients have a right to have records sent to the person or entity of their choice provided such choice is clear, conspicuous and specific, which we wholeheartedly endorse. Unfortunately the NPRM added a further requirement that the choice be in writing and signed, and even though that could be done electronically, if it is done electronically it has to be in conformity with the electronic signature requirements of each state and I doubt if any of us in the room even know what all of those are, much less the average provider. So we are greatly troubled at the idea that this will serve as an inadvertent impediment to patients being granted meaningful access to their records through PHRs and we would really encourage that policymakers to take a look at the part of the NRPM that deals with immunization requests where the rule says that if parents in
particular have properly authenticated themselves
in the health care setting, then the providers can
honor an oral request to send the immunization
records, for example, to the child's school, so
that I think in the health care setting when the
patient has properly identified themselves,
they've obtained care and so on, that at the point
of perhaps checking out or talking to their
provider if they express an oral request to have
their records sent to a destination of their
choice that we'd like to see that honored in the
interests of advancing patient access to records
through PHRs.

MS. PRITTS: Thank you. We'll now turn
back to the phone, please.

MR. HOWELL: I'm somewhat disappointed
that our government, as well, is opposed to our
looking at how we are going to scrutinize the
sharing of information in HIEs, the health care
information exchanges between payors, payees,
doctors in their physician practices. We should
have done this upfront-- because a lot of the
EHRs, HIEs, have been developed as you very well know, already, where they're already doing scrapes, extrapolating information off of a multitude of websites after the fact. Now they're trying to do once again after the fact, shoring up patient information.

MS. PRITTS: Thank you for your comment, and we will now turn back to the gentleman in the back of the room, please.

MR. CARUSO: Hello, I'm Tom Caruso and I'm building a think tank, a biomedical informatics think tank. You can find more information at tpcaruso.com. I wanted to comment about the lack of conversation concerning clinical research. The future of medicine is really being defined by researchers that are in academic institutions that could very significantly benefit from access to public health records and to mechanisms to consent those individuals who are using those public health records to participate in studies and to even pay those people to participate in some way. I would like to see more
conversation including clinical researchers and
biomedical researchers who could use this
information very significantly in improving
quality of care in various different ways.

MS. PRITTS: Thank you for your comment.
Are there any more comments on the phone, please?
[ no]. Anyone else? [no].

I'd like to thank everyone for coming.

I would like especially to thank the people who
managed to stay all day. I know it's been a very
long day. I do understand the desire for
participatory forums. We do strive to have an
open government. We have made great process I
think in this administration in making things much
more transparent in collecting comments in advance
and providing a lot of opportunities for people to
participate in these events, and so we'll take
those comments as we go forward and see what we
can do about that.

This may not be appropriate, but I'd
also like to comment back that it's important that
in these forums when you do that, that it's a
two-way process so there has to be some respect
for the process also from the participants, so
that one of the difficulties in these kinds of
forums is the lack of adherence to time. We did
not have that today, but I'm sure you've all been
in conferences when people have ignored the time
limits and not adhering to the subject matter of
the calls and things of that manner. So there are
some difficulties with doing that, but I think
this is just a general comment that should be
responded to, that it is a very useful process to
have more open dialogue and useful for us to take
that into consideration, how to make that happen
in a very meaningful way, so I deeply appreciate
that comment and it's something that I think that
we should really think about a lot more.

Having said that, I do appreciate
everybody having come and stayed particularly for
our panelists. For me this has been an extremely
informative day and I hope it was for you too.
There were a number of thoughts here today and a
number of things here today, but some of the ones
that I think that really came up, I can't possibly summarize everything that was said today, but the things that really stick in my mind for the most part are that the borders are very blurred as between what health information is and what other information is, that the mode of holding information is very blurred between what an electronic health record might be, a PHR might be and any other mode, and that it's very difficult to put boundaries around those different things and to know how to manage them.

As I started the day, I would like you leave you all with a quote. This one is not quite as old as the one I opened with which was from the 1700s. This one was from 1997 and I know in tech terms that might as well be the 1700s in some ways. It's from Donna Shalala who was speaking at the Press Club shortly after HHS issued its report to Congress when Congress was still trying to pass a kind of unified health information protection statute, which as we all know it was unable to do. The question remains pertinent today as it was
then, which is, "When all is said and done, will our health information be used to heal us or to reveal us?" And with those kind thoughts, I will leave you. Thank you very much and have a good weekend.

(Whereupon, at 4:43 p.m., the PROCEEDINGS were adjourned.)

* * * * *
CERTIFICATE OF NOTARY PUBLIC

DISTRICT OF COLUMBIA

I, Irene Gray, notary public in and for the District of Columbia, do hereby certify that the forgoing PROCEEDING was duly recorded and thereafter reduced to print under my direction; that the witnesses were sworn to tell the truth under penalty of perjury; that said transcript is a true record of the testimony given by witnesses; that I am neither counsel for, related to, nor employed by any of the parties to the action in which this proceeding was called; and, furthermore, that I am not a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

-----------------------------------
Notary Public, in and for the District of Columbia
My Commission Expires: April 14, 2011