

**HEALTH INFORMATION TECHNOLOGY: PRO-
TECTING AMERICANS' PRIVACY IN THE DIG-
ITAL AGE**

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY

UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

—————
JANUARY 27, 2009
—————

Serial No. J-111-3

Printed for the use of the Committee on the Judiciary



U.S. GOVERNMENT PRINTING OFFICE

54-240 PDF

WASHINGTON : 2010

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin	ARLEN SPECTER, Pennsylvania
DIANNE FEINSTEIN, California	ORRIN G. HATCH, Utah
RUSSELL D. FEINGOLD, Wisconsin	CHARLES E. GRASSLEY, Iowa
CHARLES E. SCHUMER, New York	JON KYL, Arizona
RICHARD J. DURBIN, Illinois	JEFF SESSIONS, Alabama
BENJAMIN L. CARDIN, Maryland	LINDSEY O. GRAHAM, South Carolina
SHELDON WHITEHOUSE, Rhode Island	JOHN CORNYN, Texas
RON WYDEN, Oregon	TOM COBURN, Oklahoma
AMY KLOBUCHAR, Minnesota	
EDWARD E. KAUFMAN, Delaware	

BRUCE A. COHEN, *Chief Counsel and Staff Director*

NICHOLAS A. ROSSI, *Republican Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Cardin, Hon. Benjamin L., a U.S. Senator from the State of Maryland	7
Hatch, Hon. Orrin G., a U.S. Senator from the State of Utah	2
Kaufman, Hon. Edward E., a U.S. Senator from the State of Delaware	5
Klobuchar, Hon. Amy, a U.S. Senator from the State of Minnesota	4
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	5
prepared statement	111
Whitehouse, Hon. Sheldon, a U.S. Senator from the State of Rhode Island	1

WITNESSES

Hahn, Adrienne, Senior Attorney and Program Manager for Health Policy, Consumers Union	12
Hester, James, Jr., Ph.D., Director, Health Care Reform Commission, Vermont State Legislature	8
Houston, John, Vice President of Information Security and Privacy, and As- sistant Counsel, University of Pittsburgh Medical Center	15
McGraw, Deven, Director, Health Privacy Project Center for Democracy and Technology	10
Merritt, David, Project Director, Center for Health Transformation and the Gingrich Group	17
Stokes, Michael, Principal Lead Program Manager, HealthVault, Microsoft Corporation	14

QUESTIONS AND ANSWERS

Responses of Adrienne Hahn to questions submitted by Senators Leahy, Specter and Hatch	35
Responses of James Hester to questions submitted by Senators Hatch and Leahy	44
Responses of John P. Houston to questions submitted by Senator Hatch	45
Responses of Deven McGraw to questions submitted by Senators Specter, Hatch and Leahy	61
Responses of David Merritt to questions submitted by Senators Hatch and Specter	64
Responses of Michael Stokes to questions submitted by Senators Leahy and Hatch	66

SUBMISSIONS FOR THE RECORD

AARP, Washington, D.C., statement	73
ACLI, Frank Keating, President & Chief Executive Officer, Washington, D.C., letter	79
American Psychoanalytic Association, James C. Pyles, Washington, D.C., let- ter and attachment	80
Coalition for Patient Privacy, Ashley Katz, Austin, Texas, letter	92
Hahn, Adrienne, Senior Attorney and Program Manager for Health Policy, Consumers Union, statement	95
Hester, James, Jr., Ph.D., Director, Health Care Reform Commission, Vermont State Legislature, statement	102
Houston, John, Vice President of Information Security and Privacy, and As- sistant Counsel, University of Pittsburgh Medical Center, statement	107
McGraw, Deven, Director, Health Privacy Project Center for Democracy and Technology, statement	113

IV

	Page
Merritt, David, Project Director, Center for Health Transformation and the Gingrich Group, statement	133
National Association of Chain Drug Stores, Alexandria, Virginia, statement ...	158
National Business Group on Health, Helen Darling, President, Washington, D.C., letter	165
Peel, Deborah C., MD, Founder & Chair, and Ashley Kats, MSW, Executive Director, Patient Privacy Rights, Austin, Texas, joint statement	167
Stokes, Michael, Principal Lead Program Manager, HealthVault, Microsoft Corporation, statement	175
Vermont Information Technology Leaders (VITL), Gregory Farnum, Presi- dent, Montpelier, Vermont, letter	183

HEALTH INFORMATION TECHNOLOGY: PROTECTING AMERICANS' PRIVACY IN THE DIGITAL AGE

TUESDAY, JANUARY 27, 2009

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The Committee met, pursuant to notice, at 9:31 a.m., in room SD-226, Dirksen Senate Office Building, Hon. Sheldon Whitehouse, presiding.

Present: Senators Leahy, Cardin, Whitehouse, Hatch, Klobuchar, and Kaufman.

OPENING STATEMENT OF HON. SHELDON WHITEHOUSE, A U.S. SENATOR FROM THE STATE OF RHODE ISLAND

Senator WHITEHOUSE. Good morning. I am sorry the Chairman is not with us at this moment. We are expecting him. But in the meantime, he has asked me to get the hearing underway. I am Senator Whitehouse from Rhode Island, and I am very pleased to have been invited to have the opportunity to chair this hearing. I will take the liberty of having the floor here to give my 2 cents on why I think this is so important.

We are on a very bad glide slope for health care in this country with a \$30-plus trillion liability just for Federal health care benefits that is totally unfunded, not a nickel against that liability. We have calculated that the Bush addition to the deficit was \$7.7 trillion before we even got around to the bailouts. And that seems like an impossibly big number. We have been arguing about \$700 billion TARP funds. We have been arguing about \$35 billion auto bailouts. Thirty-plus trillion dollars is an astonishing liability to have to face, and I believe that there are only two ways to face it.

One is with a very bloody toolbox comprised of benefits cuts, throwing people off coverage, paying providers less, and raising taxes, and we are far too far down all those roads with our health care system already. So that would be a very unfortunate toolbox to have to resort to.

The better toolbox is reform of the delivery system to make it more efficient so it is not creating so many casualties, so it is not creating so much waste and turmoil and division and stress and paperwork and duplication and waste. And in order to do that, health information technology is going to be an absolute key. The three legs of that stool, I think, are health information technology,

investment in quality and prevention, and reimbursement reform, payment reform, so that the price signals match what we want.

The health information technology platform is absolutely an essential element, not sufficient but essential, to getting that done, and I very firmly believe that the Achilles heel of health information technology is privacy. If the American people do not believe we have protected their privacy adequately, then the HIT initiative, the health information infrastructure America needs will simply not get through this building. And if it does not, that is a real tragedy because that toolbox takes about 10, 15, 20 years to fully deploy. We have got to get going now on that, and if we waste this moment, the time will come when we are only left with that bloody toolbox, because those tools, as awful as they are, have the one advantage that you can deploy them right away. And so if you have missed your moment with the reform toolbox, that is what you have left. And that is, I think, where we are right now.

So I put this privacy question at the center of the most important economic issue the country faces, and I am delighted to have the chance to hear from all these wonderful witnesses. I am delighted to have the distinguished Senator from Utah, Senator Hatch, here; the distinguished Senator from Minnesota, Senator Klobuchar, here.

Senator Hatch, would you like to make some opening remarks, sir?

STATEMENT OF HON. ORRIN G. HATCH, A U.S. SENATOR FROM THE STATE OF UTAH

Senator HATCH. Well, thank you, Chairman Whitehouse. We appreciate you and your leadership here, and I want to especially thank our panel here today. I appreciate the opportunity to say a few words on health IT this morning and, of course, welcome our distinguished panel, and especially you, Mr. Houston, from my alma mater, the University of Pittsburgh. I am pleased to have you here, and all of you.

There is no doubt that we are living in an Information Age. Technology has radically changed business and other aspects of American life, and I believe that health IT can greatly streamline the health care sector by saving costs, time, and, most importantly, lives.

I am proud to point out that Inter Mountain Health Care, which is headquartered in Salt Lake City, Utah, has been a national leader in adopting—and probably “adapting” would be a good word, too—health IT in an integrated manner and could serve as a model for other health care delivery systems across the Nation.

My colleagues and I on the Senate Finance Committee and HELP Committee have been working for some time to increase efficiency and reduce costs in our Nation’s health care industry. I believe the widespread use of health IT would undoubtedly reduce medical errors, inconsistent quality, and rising costs currently burdening the health care industry today. In fact, a Rand Corporation study projected that health IT has the potential to save the health care system billions of dollars each year.

Now, I am proud to have been a co-author of the bipartisan Wired for Health Care Quality Act, both in the 109th and the

110th Congress, along with my colleagues on both sides of the aisle, including Senators Kennedy, Enzi, and Clinton. Unfortunately, we might not have a chance to reintroduce this bipartisan legislation again in this Congress since health IT is now being addressed through the stimulus legislation.

Now, regretfully, this language was crafted without the input of Republican offices, including mine, who have demonstrated long-standing interest in this important bipartisan issue. The widespread use of health IT would allow medical data to move with people as they move. Health IT would eliminate the cost of paper claims and help spread clinical research within the medical community. We have the most advanced medical system in the world. The United States now leads the world in technological innovation, and I hope we can stay there. There is no reason why people's health files—their medical history, test results, lab records, x-rays—cannot be accessed securely and confidently from a doctor's office or hospital. And I believe we have to develop a nationwide interoperable health IT infrastructure that has strong but prudent privacy and security protections. Providers must be able to easily manage their information needs to provide coordinated and quality care delivery while securely managing the needs of their patients.

Now, I believe that the use of information technology is essential in promoting a system of coordinated and quality-focused health care in this country in the health care delivery system. I think we have to embrace cutting-edge information technologies in health care, and we cannot afford to miss this opportunity.

Now, I look forward to hearing from these witnesses here today. I might mention that Senator Specter, our Ranking Member on this Committee, is unable to attend, at least at this time, and has asked me to be sure that I attend. And, of course, as you all know, I take a tremendous interest in everything involving health care around here. So I am very interested in what you have to say and the contributions that you care to make to us to help us to understand this complicated but understandable set of issues.

Thank you so much, Mr. Chairman.

Senator WHITEHOUSE. Thank you, Senator.

The role of the States has really been impressive in all this, particularly in the absence of concerted, effective Federal leadership, and Utah, through its Utah Health Information Network and through Inter Mountain, has shown great, great leadership as a State. And I know Senator Hatch has been keenly interested and involved in those, so we are delighted that he is here.

Another State that has shown great success and leadership in Minnesota, and Senator Klobuchar of Minnesota would like to add an opening statement.

Senator Klobuchar.

Senator HATCH. Could I interrupt for a minute? We are really happy to welcome both you and Senator Kaufman to the Committee. You will like the Committee, and I think you will make great contributions. And I think both of you will help to make this Committee much more bipartisan.

**STATEMENT OF HON. AMY KLOBUCHAR, A U.S. SENATOR
FROM THE STATE OF MINNESOTA**

Senator KLOBUCHAR. Thank you so much. Well, thank you, Senator Hatch for that. Thank you, Mr. Chairman, for your leadership on this issue. As you can see, serving as both the junior and senior Senator from my State has somewhat weakened my immunity system, so I have a cold. But it has not weakened my resolve to serve on this Committee. So I am very excited to be here. I served for 8 years as the Hennepin County attorney in Minnesota, where I was a prosecutor, but I also represented one of the biggest hospitals in our State, Hennepin County Medical Center. So I have a lot of familiarity with some of these issues, although when I think of the technology issues, which Senator Whitehouse has so well talked about on the floor and showed such leadership on, actually my real memory is of two things.

One is when I had my hip problems; I had my hip replaced at some point at Mayo Clinic. Driving around with multiple x-rays by myself in the back seat of my car where they got hot and one of them almost melted, I thought there must be something better we could do with health care in the country.

The second was that one time when I was county attorney trying to get all of our police departments to change their complaint forms so that they were routine and we could put them in the computer at the same time. And I went to one of the smaller departments, and they said, "We cannot do that. We just bought new file cabinets, and they only fit one kind." And I think of this all the time when I think of the great challenge it is to try to get institutions to change their technologies so that they match.

It is incredibly important in the health care area. A study published last year in the New England Journal of Medicine found that only 4 percent of U.S. physicians were using fully functional electronic record systems, and missing medical records occur in one of every primary care visits. Serious medical errors that come as a result of missing records are costly, time-consuming, and preventable. With the U.S. spending \$2.3 trillion per year on health care, we must bring an end to the inefficiencies of the system, and if implemented thoughtfully and with the kind of balance that I hope we talk about here today, health information technology has the potential to reduce waste, improve quality, and stimulate innovation.

No information is more private than an individual's health information, and despite federally mandated privacy protections, consumers continue to have concerns about the privacy of their records. And I would agree with Senator Whitehouse that this is one of the major issues, intentions we see as we try to implement better medical technology.

If we are going to achieve the savings we would like to see with medical technology, we must work to develop regulations and laws that inspire consumer confidence and trust. As with other industry advances in information technology, consumer confidence is achieved with proper security protection and improvements in business practices. Health IT investment must be designed to achieve modernization and measurable health outcome improvements. In Minnesota, we are leading the way for health care innovation.

Countless hospitals from Winona to Duluth have been recognized for the measured quality outcomes that have resulted from effective information technology.

We have also led the way in ensuring that the privacy of the patient remains protected. Patient consent is required in my State for nearly all disclosures of health records, and it is one of the few States that gives citizens a private right of action if the privacy of their medical records has been compromised.

I am interested in learning from all of you what providers, consumers, and businesses are doing to help ensure the advancement of technology in our health care industry, while still working to provide the privacy and security of our patients.

Thank you very much.

Senator WHITEHOUSE. I am delighted to join Senator Hatch in welcoming Senator Klobuchar to the Committee. We were classmates, and we have spent a lot of time together. We sit next to each other on Environment and Public Works, and it is wonderful to have her join us on Judiciary as well.

Senator Kaufman, in addition to being a new member of the Committee, is also a new Senator representing the great State of Delaware. We are delighted to welcome him and ask him to make an opening statement.

**STATEMENT OF HON. EDWARD E. KAUFMAN, A U.S. SENATOR
FROM THE STATE OF DELAWARE**

Senator KAUFMAN. Sure, I just have a few comments.

First, I want to thank Senator Hatch, and I do want to operate in a bipartisan manner, as you have over the years with my former Senator, Senator Biden.

I just have a few comments I want to make in the beginning. First, thank you for coming here. This is really an important issue. Everywhere I travel in Delaware, people are concerned about the privacy of their medical records, and everywhere I travel around here, people are concerned about the exploding costs of health care. So we have this kind of conundrum on how we are going to move forward on these two areas. And the main areas I am interested in today is kind of we are coming up with a very major bill, the Economic Recovery Act, and there is going to be a lot there, hopefully some things in health care that are going to help. But we want to make sure there are not things in there that are going to hurt.

So I am looking forward to your testimony, and I am looking forward to the hearing. Thank you.

**STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR
FROM THE STATE OF VERMONT**

Chairman LEAHY. Thank you very much, Senator Whitehouse, for being here. I apologize for being late. It certainly is not the weather. As Dr. Hester knows, we do not let weather like this bother us in Vermont. Anything under 5 inches is considered a dusting, at best. And with a Minnesotan and, Senator Hatch, you get snow out in Utah, don't you.

Senator HATCH. We have been known to have snow.
[Laughter.]

Chairman LEAHY. I think you measure by the foot on occasion. I am delighted to see our new members here, Senator Klobuchar and Senator Kaufman. I must say that Senator Klobuchar, like me, is a former prosecutor, and Senator Kaufman probably understands this Committee better than I or anybody else here, the years he has spent here. So thank you.

I had a delay in the doctor's office before coming here. That is what held me up, which is interesting because we are talking about how you protect Americans' health privacy rights. We are going into a national health IT system, which I strongly support the idea. I think you have to have innovation in American health. That is the only way we are going to make sure that we get health to everybody, but we also bring the costs down.

I am pleased that President Obama has called for the immediate investment in health information technology. If it works the way we want, Americans' medical records will be computerized within 5 years.

Today, if you have a health record, you have a health privacy problem. My wife is a registered nurse, now retired, but she used to tell me how concerned she was to see health records around the hospital. Now you have electronic health records, digital data bases, and the Internet, and we have to protect people's privacy in that.

If you can just click on a mouse and pull up records, that can obviously be helpful for cost-effective health care, but you have to make sure that personal privacy is protected. And if you do not have adequate safeguards to protect health privacy, many Americans are not going to seek medical treatment, which we have to worry about, because they fear that their sensitive health information will be disclosed without their consent. And those who do seek medical treatment assume the risk of data security breaches and other privacy violations. And health care providers who think there are privacy risks, they are going to see that as inconsistent with their professional obligations, and they will not want to participate.

So it becomes the good news/bad news. The good news, it is a very great thing if we can do it; the bad news, if there are leaks in there, health providers will not want to use it and patients will not want to use it.

Now, as Dr. Hester knows, in my home State of Vermont, we have formed a public-private partnership that is charged with developing Vermont's statewide electronic health information system, including a policy on privacy. I think that in order for a national health IT system to succeed, we in Congress should follow Vermont's good example and work together with public and private stakeholders to ensure the privacy and security of electronic health records. I have worked for more than a decade with Senator Kennedy—a tireless champion of health IT—and many other Members, both Republicans and Democrats, on this.

I think some have suggested that addressing privacy in health IT legislation is too hard and that we should put that issue off for another day. I disagree. If you do not have meaningful privacy safeguards, you are not going to get a health IT system.

In his inaugural address, President Obama eloquently noted that in our new era of responsibility “there is nothing so satisfying to

the spirit, so defining of our character than giving our all to a difficult task." This is a difficult task. Americans are up to it. The Congress had better be up to it. And we will make it.

So, Mr. Chairman Whitehouse, I appreciate this, and I will stay and listen to the witnesses. I understand that Senator Hatch and Senator Klobuchar and Senator Kaufman made opening statements. Did you and Senator Cardin? And I must say that Senator Cardin is from the great State of Maryland, and we love Maryland. I have two grandchildren who live in Maryland, plus the parents, of course.

Senator CARDIN. The roads between Baltimore and Washington were very clear today. Maryland did a good job in cleaning the roads, in case you are wondering. I got here on time.

Chairman LEAHY. And your wonderful hospital, Johns Hopkins, saved my wife's life, so I appreciate it. Go ahead.

**STATEMENT OF HON. BENJAMIN L. CARDIN, A U.S. SENATOR
FROM THE STATE OF MARYLAND**

Senator CARDIN. Well, thank you. I appreciate you mentioning that because we are very proud in this country of the quality of health care. This Nation leads the world in medical technology, and we are proud of the quality of care that some people, most people in this country can receive, but too many people are denied access to care because of the high cost of health care in America and because of the large number of people who do not have any third-party reimbursement for health care. And we needed to do something about that, and I agree with President Obama, who has made health care reform one of his top priorities. And as part of that, it is to have a much more cost-effective system as far as medical information and administrative costs are concerned.

I think we all agree with that, and I agree with the Chairman's comments about the goal that we clearly have of using information technology much more efficiently in this country so that those who are providing health care can get the necessary information to provide quality care and to avoid mistakes, and that all becomes a very important part of our health care system.

I do first want to acknowledge Senator Klobuchar and Senator Kaufman and welcome them to the Judiciary Committee. It is wonderful to have both on our Committee, and I think we will have Senator Wyden for at least a short period of time on our Committee, maybe longer. But it is nice to have our new members, and we welcome them. Senator Klobuchar is not a new Member of Congress. We came to the Senate at the same time. And Senator Kaufman, as the Chairman has already alluded to, had a great deal of experience, more than I think any other member of this Committee, and we welcome your help as we try to deal with some very complicated issues, including how to deal with protecting privacy and allowing us to have an efficient system for sharing of information.

And I just want to make an observation. I served on the Ways and Means Committee for a number of years and was involved in privacy issues in health care. I think part of the problem is that those who collect health care information have not been as selective as I think they should be in trying to get consent from their pa-

tients on sharing of information, because in many cases this information does not need to be shared, or it could be stored in a way that is encrypted or protects the personal identity of the individual, and yet in so many cases the collector of the information decides not to put it in that format because of whatever reason.

So I do think we have to use some common sense here as to how we can protect the privacy of the information and avoid the coercive practices that health care professionals can use in order to get waivers, including denying care unless you sign those forms, which do not have a lot of meaning to people who are stressed about getting health care. They are not going to read the information on signing the waivers.

So we have to come up with a better system to really have informed consent, because I think it is critically important that those who use our health care system know that their personal information will not be shared without their informed consent. And we have to come up with a way to figure out how to do that.

So, to me, this hearing is critically important as we try to make sure that we do have a system that is efficient and one that allows health care professionals to have immediate access to information that they need in order to properly treat their patients, but at the same time avoid the intentional or the negligent release of medical information that can compromise not only the rights of individuals, but their confidence that our system is doing it in the right manner.

Thank you, Mr. Chairman.

Senator Whitehouse. Thank you.

We will now hear from our learned panel. We are very proud to have you with us, and we will begin with Dr. James Hester, who comes to us from the Chairman's home State, the great Green Mountain State of Vermont, where he is the Director of the Health Care Reform Commission for the Vermont State Legislature. With 35 years of experience in the health care field, he has held senior management positions with MVP Health Care in Vermont, Choice Care in Cincinnati, Pilgrim Health Care in Boston, and Tufts New England Medical Center in Boston.

Dr. Hester earned his Ph.D. in urban studies and his M.S. and B.S. degrees in aeronautics and astronautics, all from the Massachusetts Institute of Technology. He also holds a Master's of Education degree from St. Michael's College, and we welcome him to the Committee.

Dr. Hester.

**STATEMENT OF JAMES HESTER, JR., PH.D., DIRECTOR,
HEALTH CARE REFORM COMMISSION, VERMONT STATE
LEGISLATURE**

Mr. HESTER. Thank you, Mr. Chair. Thank you for the opportunity to testify on this critical issue. I think my testimony will be supportive of several of the themes that the opening remarks of the Committee have made. My testimony today does not reflect the official positions of the legislature or the commission. I want to be clear about that.

I come before you not as a privacy expert or IT expert but, rather, as one with extensive experience in using information and infor-

mation technology as a means to furthering effective health care reform.

Health care reform in Vermont, which has been underway for almost 8 years, is the most comprehensive State initiative in the country, built on an integrated strategy which includes:

One, expanding affordable coverage in a sustainable way. We reduced the uninsurance rate in the State from 10 percent to 7.5 percent in the last 2 years in the face of a declining economy.

Second, bending the medical cost curve by improving the prevention and treatment of chronic illnesses. Our Blueprint for Health has pilot programs in three Vermont communities covering 10 percent of the Vermont population, which is showing some great results on this.

And, finally, using information technology as a catalyst for performance improvement. Sustainable improvements in coverage and chronic illness care can only be achieved with the support of information technology. It is impossible to obtain the desired performance of our health care system as long as key clinical information is only available to providers and patients through paper charts sitting in filing cabinets.

As mentioned, the primary vehicle for our IT strategy has been VITL. It is a new public-private organization. In the last 3 years it has completed a State Health IT plan, implemented several pilot programs, and begun building the core infrastructure for the statewide health information exchange.

Last May, Vermont became the first State in the country to provide the long-term financing to pay for both the development of the statewide Health Information Exchange Network and for electronic medical records for all independent primary care practices in the State.

This transition from creating a plan and implementing relatively small-scale pilots to full-scale statewide implementation has provided a major impetus for the review of the privacy and security policies. Those efforts are in their final stages, but are now on hold pending clarification of the proposed privacy guidelines in the economic stimulus act.

While the health IT financing goes far toward reducing the financial barrier to widespread implementation of health IT, it is not sufficient by itself. Realizing the benefits of health IT requires broad acceptance by both patients and providers of this new technology which deals with the most sensitive types of data. The process that VITL has engaged in represents a delicate balancing act between sometimes conflicting interests of consumer control and needs and provider accountability and responsibilities. Unless consumers are confident that their information is secure and will be used appropriately, they will not participate in electronic health information exchanges. Unless providers believe that the administrative burdens are reasonable and the information is reliable, they will not participate in such exchanges either.

Moving forward with our health care reform totally depends upon finding an initial balance point between conflicting needs and interests in a way which will encourage broad-based participation of patients and providers. I am confident that once the Federal privacy guidelines and requirements in the stimulus act are finalized,

VITL will be able to rapidly complete the revision of its guiding principles and operating policies.

However, this balance point is not static; it will evolve. We fully expect that the implementation of the initial privacy policies in a steadily growing set of pilot health reform initiatives will teach us important lessons over the next couple of years. We will have to return to these policies on a regular basis to update them based on what we have learned and new technical capabilities. The core security and privacy capabilities have been carefully thought through, however, and provide a sound foundation for beginning this expansion.

Vermont health care reform is built on scalable, community-level pilot programs which enable us to learn rapidly what works and what needs to be improved. We will use this model to evolve our privacy and security policies and capabilities as well.

Given the strong feelings surrounding protected health information and the uncertainties that are inherent in the early stages of the spread of EMRs, I fully expect that a significant minority of both patients and providers may elect not to participate. A reasonable goal is to devise a program which will satisfy the needs of a large enough percentage of users to enable robust testing of capabilities, deliver value to the users, and drive the next round of privacy and security technology. As capabilities mature and confidence grows, the hope and expectation is that our program will earn the trust of a steadily expanding percentage of both our population and the health care delivery system. The successful scaling up of our pilot programs into systemwide initiatives and the long-term success of our health reform efforts depend on it.

[The prepared statement of Mr. Hester appears as a submission for the record.]

Senator WHITEHOUSE. Thank you very much, Dr. Hester.

Our next witness this morning is Deven McGraw. She is the Director of the Health Privacy Project at the Center for Democracy and Technology. Prior to joining CDT, she was an associate in the public policy group at Patton Boggs LLP and in the health care group at Ropes & Gray. Ms. McGraw received her bachelor's degree from the University of Maryland. She earned her J.D. and L.L.M. from Georgetown University Law Center. She also holds a Master of Public Health degree from Johns Hopkins School of Hygiene and Public Health. We welcome her to the Committee.

Ms. McGraw.

STATEMENT OF DEVEN MCGRAW, DIRECTOR, HEALTH PRIVACY PROJECT, CENTER FOR DEMOCRACY AND TECHNOLOGY

Ms. MCGRAW. Thank you very much, Mr. Chairman, members of the Committee, and thank you for holding this hearing today. It really could not be more timely or more important. We have economic recovery legislation on the table that has \$20 billion, at least—depending on what you are looking at—to promote the adoption of health IT, and this commitment is really laying the building blocks for health reform. It is going to help us create the information superhighway for health that will improve health care quality and engage more consumers in their care.

This is very good news. It is an important opportunity, and surveys consistently show the support of the American public for health IT. But these very same surveys also show that the public is concerned about the risks to their privacy when medical information will be moved online. A system that makes greater volumes of information available for the right purposes—to improve our care—is also an attractive target for people who would seek it for commercial gain or for other inappropriate purposes. So building trust in these systems is absolutely critical to realizing the benefits of this technology.

Some say that privacy is an obstacle to achieving a digital health system. As Senator Leahy mentioned, it is not always easy to figure out the right way to approach this. But, really, it is not an obstacle. In fact, the opposite is true. Enhanced privacy and security built into health IT will bolster consumer trust and spur the more rapid adoption of health IT and, therefore, allow us to realize these benefits.

So a commitment to spending significant dollars to advance health IT must be coupled with a strong commitment to privacy and security. One without the other is a job half done and will set us back significantly.

Congress' role is critical here, and strong privacy protections must be part of any legislation that moves health IT. We cannot do this later. We will not have another opportunity.

We have taken on privacy once before in HIPAA, but health care is really rapidly changing, and the way we move information today is different than it was then, and it is going to be even more different tomorrow and in the decades to come. So we really need a second generation of health privacy, a comprehensive, flexible privacy and security framework that sets clear rules for who can access personal health information and for what purposes that apply to all entities that are engaged in e-health.

The bill that is pending builds on HIPAA and takes some concrete steps forward to the realization of this comprehensive framework of protections, and we support them. They are like a down-payment, a good first step. But hopefully this will not be the last opportunity for us to talk about this. As Dr. Hester aptly pointed out, you know, these conversations are going to—you know, making sure we get this right is going to require an ongoing commitment from Congress, the administration, and the private sector as well.

In my testimony I have some detail about the privacy provisions that are in the stimulus package, at least the ones that I have seen in the House bill that got marked up the other day, and so I will just touch on a few. It includes Federal right to be notified if your health information is breached; giving patients a right to an audit trail of disclosures from their medical record; ensuring that records or data cannot be sold or used for marketing purposes without your authorization. It has provisions to improve enforcement. It tasks the HHS and the Federal Trade Commission to work to develop protections for personal health records, which are consumer-based tools which require a different set of protections. Again, my testimony has details on all of that.

I will close by saying, you know, the other thing that Congress might do is to task the Secretary with ensuring that all entities

adopt and implement both policies and technological solutions that address fair information practices of data stewardship, then hold funding recipients accountable for how they implement privacy protections. At the end of the day, whatever happens in the stimulus and having HIPAA, some folks will be covered adequately; some folks will not. Having the private sector develop policies will give us that extra measure of safeguard, and I think that if I were going to add one more thing to what is already a very strong package of protections, that would be it.

Thank you for the opportunity to testify today, and I am happy to answer any questions you might have.

[The prepared statement of Ms. McGraw appears as a submission for the record.]

Senator WHITEHOUSE. Thank you, Ms. McGraw.

Our next witness is Adrienne Hahn. She is a Senior Attorney and Program Manager for Consumers Union. As a health care advocate, Ms. Hahn is an expert on medical privacy, health care financing, Medicaid, and patient safety efforts at the Federal level. Previously, Ms. Hahn served at the United States Department of Justice as an attorney in the Civil Rights Division. She earned her Bachelor of Arts degree from the Colorado College—where she was a classmate of my sister—and her J.D. from Boston College Law School. We welcome Ms. Hahn to the Committee.

STATEMENT OF ADRIENNE HAHN, SENIOR ATTORNEY AND PROGRAM MANAGER FOR HEALTH POLICY, CONSUMERS UNION

Ms. HAHN. Thank you. Mr. Chairman and members of the Committee, thank you for inviting me to testify today. Consumers Union is the independent, nonprofit publisher of Consumer Reports magazine, and we work on a wide range of health care.

There is widespread agreement to accelerate the use of health information technology in our otherwise high-tech health care system. Most hospitals and doctors' offices still store patient records on paper, making the history of medical care hard to transfer from one hospital to another or one doctor to another. The inefficiencies of this system can lead to medical errors and the loss and misplacement of vital information. As for patients, we rarely see our own fragmented records or track our own health histories.

Consumers Union, therefore, strongly supports the movement toward an electronic system of health records and information exchange. By harnessing the power of modern information technology systems, we can improve the quality of American health care and moderate health care costs by the following: one, reducing errors; two, eliminating service duplication; three, promoting pay for performance; and, four, providing the data necessary to evaluate the actual comparative effectiveness of various treatments and drugs.

A national system of electronic medical records has the potential to improve the quality of health care by reducing hospital-acquired infection rates. Through a network of electronic medical information, families can identify the safest and the highest-quality hospitals. As just one example of the tremendous improvements in quality and cost savings that are possible, Consumers Union has been conducting a national campaign to promote the disclosure of

hospital infection rates, and you can find out more information about that at www.StopHospitalInfections.org.

Each year, there are about 2 million patients who acquire infections in hospitals and about 100,000 who die. In 24 States, we have worked with State legislatures to pass laws to require hospitals to report their rate of infection based on the idea that public disclosure will prompt hospitals to adopt effective methods to reduce their infection rates. Electronic medical records technology and the public disclosure of more types of patient care data where the patient is not identified will make it easier for consumers to reward those who provide quality.

While there can be important public and private benefits of creating an effective electronic medical records system, we believe polls demonstrate that quite effectively. From the great potential of such systems unless more is done now to ensure privacy, there will not be the heart and soul of the American public in order to support that. In short, this requires enabling patients to participate in deciding when, with whom, and to what extent their personally identified medical information is shared.

It is important that we all recognize that there is no hack-proof database or system, and once more medical data is moving electronically, it is subject to threats from hackers, identity thieves, and others. That is simply a fact of life, reconfirmed almost daily by new stories of financial and medical record data violations.

Beyond the likely scenarios of security breaches, the value of electronic health information is such that many organizations will want to exploit secondary data sources for private financial gain, rarely—if ever—with patient knowledge, let alone consent. It is imperative that policymakers take aggressive steps to protect privacy. Otherwise, security breaches could doom expanded use of health information technology.

Additionally, some will say that it is too complex or it is too expensive to allow people to control their medical information. Computers have the ability to handle the task. They have been designed to deal with huge numbers of variables—like 50 State laws—and to create special files where certain data are only available to a designated provider on a “need-to-know basis.” If we do not meaningfully address the privacy issue, polls show the public will not trust this system, and many will go to “off the grid” to get medical care, and we will just increase public cynicism about big Government and big business controlling our lives. In an age when the talk is of consumer-driven health care and ownership and empowerment, forcing people to share their most secret personal medical information is not the path to take.

Therefore, Consumers Union, along with a variety of different organizations, has joined an e-health initiative which includes AARP, AFL-CIO, and other organizations that support this. And we have developed a set of principles that achieve an effective balance between promoting HIT and systemic privacy safeguards. Those safeguards and protections are attached to my testimony. I would really encourage you to take a look at those. I think they provide an excellent framework to ensure that as we move down the road of health information technology, we ensure that the medical privacy records of consumers are well protected.

Thank you.

[The prepared statement of Ms. Hahn appears as a submission for the record.]

Senator WHITEHOUSE. Thank you, Ms. Hahn. We appreciate you being with us.

Our next witness is Michael Stokes, the Principal Lead Program Manager for Microsoft's HealthVault team. In this role, he is responsible for policy compliance relating to privacy across Microsoft's Health Solution Group and Advanced Research and Strategy Group. Before joining Microsoft, Mr. Stokes worked with the Hewlett-Packard Company where he designed and provided architectural business development and strategy. Mr. Stokes earned a Master's of Science from the Rochester Institute of Technology and a Bachelor of Science in Mathematics from the University of Texas at Austin. We welcome his testimony.

Mr. Stokes.

STATEMENT OF MICHAEL STOKES, PRINCIPAL LEAD PROGRAM MANAGER, HEALTHVAULT, MICROSOFT CORPORATION

Mr. STOKES. Thank you, Mr. Chairman and distinguished Senators. I am a Principal Program Manager in Microsoft's Health Solutions Group. I am accountable to ensure that our products are in compliance with applicable regulations and corporate policies, including privacy. I am honored to share my Microsoft's views on the importance of privacy in health IT. We commend the Committee for holding this hearing today and for your efforts at the intersection of privacy, information, and health care reform. Microsoft's products, including HealthVault for consumers and Amalga for hospitals and health care systems, focus on improving health care outcomes.

We recognize that health data needs to be exchanged back and forth so that everyone—patients, hospitals, providers, and clinicians—have the right information at the right time to get the best health outcomes.

We also understand that everyone, from patients to clinicians, will only be comfortable sharing health data and using health IT if they trust that that data is protected. There are three components to this trust: transparency, control, and security.

First, transparency. Participants in the health care ecosystem should be transparent about their data collection, use, and disclosure practices. If patients do not understand what data is being collected, who has access to it, or what it will be used for, they may decide not to provide any information at all, even to their own physicians. Health care providers need transparency, too, so that they understand how health data is used, how it is protected, and how their data will be disclosed to other third parties.

Second, control. Patients and other health care participants should be given control to manage health data effectively. Control allows patients to decide when and under what conditions they want to share health data. Control can help ensure that the patient's health data is shared only with the health care professionals who need to see it, and that the patient's data is not inadvertently misplaced or deleted.

Third, security. The security of health data must be protected. Concerns about potential misuse of personal data threaten to erode confidence in digital health solutions. Stakeholders will be more willing to adopt the innovative health IT solutions that can improve care and reduce costs if they feel confident that their data is secure.

By following these three principles of transparency, control, and security, we can encourage greater adoption and use of health IT and bring real change to our health care system.

Consumers will receive better information about appropriate treatments, medications, nutrition, and exercise. Health care professionals will see a more complete picture of their patients' health, allowing them to eliminate unnecessary procedures, avoid harmful drug interactions, and concentrate on providing better quality care. And researchers can discover new therapies, new breakthroughs, and new cures.

The principles of transparency, control, and security underlie Microsoft's approach to its health IT products. At the same time, we recognize that technology is only a part of the comprehensive approach to improve our health care system. Education, leadership in health care organizations, and meaningful public policy are also critical components to this success.

We look forward to partnering with you and all participants in the health care ecosystem to move forward toward a dynamic, trusted, and patient-centric health care solution system.

Thank you for the opportunity to testify, and I look forward to your questions.

[The prepared statement of Mr. Stokes appears as a submission for the record.]

Senator WHITEHOUSE. Thank you, Mr. Stokes.

Our next witness is John Houston. He is the Vice President of Information Security and Privacy and Assistant Counsel for the University of Pittsburgh Medical Center. In 2002, Mr. Houston was appointed by the Secretary of the U.S. Department of Health and Human Services to the National Committee on Vital and Health Statistics. He holds a Bachelor of Science degree in Computer Science and History from the University of Pittsburgh and a J.D. from the Duquesne University School of Law.

Mr. Houston, welcome.

STATEMENT OF JOHN HOUSTON, VICE PRESIDENT OF INFORMATION SECURITY AND PRIVACY, AND ASSISTANT COUNSEL, UNIVERSITY OF PITTSBURGH MEDICAL CENTER

Mr. HOUSTON. Thank you very much. I am grateful for the opportunity to address this Committee today regarding this important topic. I would like to start my comments by stating that the adoption of health care information technology is one of the most significant health care initiatives that this Nation can undertake. However, the widespread adoption of health IT will not be successful if our patients' privacy expectations are not met.

I am proud to say that UPMC has one of the most progressive and longstanding programs for the development and deployment of health IT in the world. Having been accountable for both privacy and information security at UPMC for the last 8 years, I am not

only aware of the public policy considerations underlying privacy and information security, but also the operational balance between a patient's right to privacy and providing timely and complete information that is necessary for the delivery of effective health care. Unfortunately, this balance is neither precise nor clear. I have seen firsthand how information barriers established in the interest of privacy have detrimentally affected patient care.

I have reviewed the current draft of the privacy legislation included in the Health Information Technology for Economic and Clinical Health Act. While the act attempts to address the evolving privacy and security requirements that have arisen since the implementation of HIPAA, it falls short of providing the necessary comprehensive and workable framework that we now need.

As the act is now being considered, I believe it is important to raise a number of concerns regarding the privacy and security provisions in the act. These concerns are more fully discussed in my written testimony, but I will highlight just a few.

Accounting of disclosures. The act provides that a patient is entitled to receive an accounting of disclosures of who accessed the patient's electronic record, even if such access was for treatment, payment, or health care operations. For an inpatient encounter, it would not be uncommon for more than 200 people to have access to various aspects of a patient's record. In practice, this could result in substantial and costly efforts on behalf of the provider with little or no apparent benefit to the patient.

Health care operations. The act provides that the Secretary will propose limitations on the use of identifiable health information for health care operations purposes. The burdens associated with de-identifying patient information must be considered, not only in terms of the effort and time associated with performing the de-identification, but also in terms of the likelihood that a covered entity will simply choose not to perform important health care operations.

Fund raising. The act provides that fund raising would no longer be considered to be part of health care operations. In difficult economic times and in an era of shrinking reimbursements, fund raising is of critical importance to most providers. Any restriction on fund raising will further frustrate a provider's ability to deliver quality health care.

Non-covered entities. The act attempts to address PHR providers, Health Information Exchanges (HIE), Regional Health Information Organizations, and other entities that had historically fallen outside the coverage of HIPAA. However, the act's treatment of each is neither comprehensive nor consistent. Rather than establishing an inconsistent privacy patchwork, a single framework needs to be established to accommodate not only today's requirements, but which also can be extended to cover the rapidly evolving health IT environment.

Enforcement. While there has been much criticism of the current enforcement strategies, I believe that the manner in which enforcement is currently performed has been effective. The act must ensure that the opportunity to collaborate continues to exist for those covered entities that are dedicated to protecting patients' privacy.

With that, I will close my comments. Thank you.

[The prepared statement of Mr. Houston appears as a submission for the record.]

Senator WHITEHOUSE. Thank you very much, Mr. Houston.

Our final witness this morning is David Merritt. Mr. Merritt is a Project Director at the Center for Health Transformation and the Gingrich Group. Mr. Merritt leads the center's projects on health information technology and expanding coverage to the uninsured. He earned his Master's degree in Political Science and Government from Loyola University, Chicago, and he earned his Bachelor's degree from Western Michigan University. We happen to know him as the editor of "Paper Kills," a book that Mr. Gingrich provided an introduction for, and he has helped Mr. Gingrich co-author an article with me on health information technology—which proves that this is an issue upon which people at opposite ends of the political spectrum can find agreement.

Mr. Merritt.

STATEMENT OF DAVID MERRITT, PROJECT DIRECTOR, CENTER FOR HEALTH TRANSFORMATION AND THE GINGRICH GROUP

Mr. MERRITT. Thank you, Mr. Chairman, and thank you for the opportunity to testify this morning.

Privacy cannot be compromised. But neither can we compromise progress in pulling our health care system out of the technological Stone Age. We need to find the right balance between privacy at all costs and progress at any cost.

One of the key ways to any of this is by creating a common, uniform framework to securely store and transmit personal health information. The Healthcare Information Technology Standards Panel, known as HITSP, and the Certification Commission for Healthcare Information Technology, known as CCHIT, are doing just that. HITSP has finalized a series of technological standards to protect privacy, and there are two that are worth highlighting.

The access control standard allows for the secure authorization to personal health information, including role-based, entity-based, and context-based access control.

The consent direct standard allows for the management of consumer rights as to who may access, collect, use, or disclose personal health information.

These standards were recently recognized in the Federal Register, meaning that any future procurement of a health IT system by the Federal Government must include these protections. Now it is up to the IT vendors to actually implement them in their products, and one of the ways to drive this is through the certification process.

Now, in full disclosure, I am on the Board of Commissioners for CCHIT, but these views are my own and do not represent the Commission.

CCHIT certifies a range of products, including electronic health records, to ensure that they meet functionality, interoperability, and security standards. There are about 50 security standards, including the two that I mentioned before, that, to be certified, an electronic health record must meet 100 percent of them.

Now, on a general note, policymakers are currently debating the future of these two organizations, and I cannot say it in stronger terms that replacing these organizations now or confusing the marketplace by creating parallel entities would literally turn the clock back 5 years, when this discussion first started. They can certainly be improved, but I think that we will pay a huge opportunity cost in time and resources if we revisit this debate now.

Now, on the broad policy proposals that are under consideration by this Committee and others, Speaker Gingrich has a belief that when you are presented with an idea, you should say “yes, if” rather than “no, because.” And I have tried to do that with some of these proposals on the table.

Yes, I think there should be an individual right of consent. Consumers should be able to opt out of certain products, services, or notifications, and they should be able to specify how their identifiable information can be shared outside the course of treatment or payment.

Consent must be balanced with health services research. I am a strong believer in the power of data. It can reveal which treatments work, which treatments do not work, the effectiveness of drugs, devices, and other vital information that really does benefit all of us. This is impossible to do without de-identified data, and when all identifiable markers are stripped, personal privacy is indeed protected.

Yes, patients should be notified of egregious breaches of privacy, but these protections should incorporate risk-based notification so that physicians, health plans, health systems, and others do not notify patients for harmless or inadvertent data sharing.

Yes, patients should have a private right of action for extreme breaches of privacy. We need to strike the right balance so that Federal, not State, litigation is available for patients, but only for clear, egregious cases.

In conclusion, we can find the right balance between privacy and progress if we are careful, judicious, and realistic. And I think once we do, we will have succeeded in transforming health care into a system that saves lives, saves money, as well as protects privacy.

Thank you.

[The prepared statement of Mr. Merritt appears as a submission for the record.]

Senator WHITEHOUSE. Thank you, Mr. Merritt. For questions, we will now turn to the distinguished Chairman of the Committee, Senator Leahy.

Chairman LEAHY. Thank you. Thank you very much, Senator Whitehouse.

Dr. Hester, I understand that Vermont Information Technology Leaders, or VITL, already have some successful pilot programs connecting electronic health records. Is that correct?

Mr. HESTER. That is correct.

Chairman LEAHY. Given your experience with that, do you agree that—basically the feeling that I have—and tell me if you disagree, of course, but that we have to have consumer confidence in the privacy of those records if we really expect them to take part in it?

Mr. HESTER. I would agree we absolutely have to have consumer confidence, and I think it is important to differentiate between the

different levels of use of the information. For example, we have a pilot that provides medication history to patients who are in the emergency room so that the physicians in the ER will know what medications have been filled in the last year. Even in that situation, where it is very contained, very specific, and there is immediate need, we still find 5 percent, 3 to 5 percent of the people do not agree, do not give the consent.

Chairman LEAHY. Even though they might be unconscious when they come in?

Mr. HESTER. You can break the glass if they are unconscious. There are provisions on that.

Chairman LEAHY. Okay.

Mr. HESTER. At the other end of the spectrum, when you start having electronic medical records which are not just being used by the practice, by the providers within a specific practice, but are connected into a regional health information exchange, the anxiety level and the requirements for earning the trust go up dramatically because the people just do not know who is involved in that.

So we have a survey of the population of Vermont. Half the population of Vermont said that in that situation they really felt it was imperative that they could control or shape who gets their information through that network.

Chairman LEAHY. Well, let me ask the same question of Ms. McGraw and Ms. Hahn and Mr. Stokes. Do you find the same thing, that you have to have consumer confidence in the privacy, if this is going to work?

Ms. MCGRAW. Absolutely, Senator. I think that if there has been a consistent theme at this hearing, it has been that if people do not trust these health IT systems that we are trying to build, we will have spent a lot of money for naught.

Now, there has been also a lot of discussion at the hearing about the role of patient consent or control as a privacy protector, and I think the only thing that I would add is that that is an important component of privacy protection. But we cannot use patient consent as the sole protector of information. We cannot rely on the individual to read a form and completely understand all of the potential uses of their information, especially when you are talking about core health care functions, like treatment or payment or the administrative tasks that are core to getting those things done.

Now, when you are talking about participation in networks, that is another story. That exposes people's information to more players than is the case when they go in to see their doctor. We actually published a paper just yesterday on what we think the right role is for patient consent.

Chairman LEAHY. If we were to put this medical IT in the stimulus bill, should we also have patient protections in there, too?

Ms. MCGRAW. Yes, absolutely. And, in fact, the bill does take concrete steps toward the protections, again, looking at a set of rules.

Chairman LEAHY. Dr. Hester, do you agree?

Mr. HESTER. Agreed that it is an essential part of that bill.

Chairman LEAHY. Thank you. Ms. Hahn.

Ms. HAHN. I would just echo what was said in terms of the concern that their medical information is private. But I would just add one other—

Chairman LEAHY. Is your microphone on?

Ms. HAHN. I would just add one other factor to that, and that is that what we have been able to look at in terms of the data, it shows that, for instance, the lack of confidence regarding medical privacy actually differs based on race as well. So what concerns us, as we know, when the United States moves to 2032 where minorities will be the majority, if this issue is not addressed appropriately now, we are actually going to be able—all the promise in terms of care coordination, quality of health care, might actually come to demise because of the fact that the minority population right now really does not trust in the information being able to—

Chairman LEAHY. So that is what your polling finds, the minority population does not trust it.

Ms. HAHN. No. We would say that there is a real concern for Americans generally, somewhere around 56—

Chairman LEAHY. But you said there was a different level of distrust—

Ms. HAHN. Oh, yes. So if you break down that data and look at it in terms of race, it actually increases in terms of the level of distrust. To give you an example, even the chronically ill have greater trust in information remaining private as opposed to an African American or a Latino. So I think that there are some real issues here in terms of we are going to be bringing all Americans along in ensuring that we provide the type of privacy protections that people have confidence in it.

Chairman LEAHY. Mr. Stokes, do you agree or disagree with what you have heard?

Mr. STOKES. Thank you for that question, Senator. As I testified, our products are dependent upon consumer trust. We believe that without consumer trust in the system, they will not adopt the system.

We also, through extensive discussions and interviews, believe this is just as important for the providers. If the providers do not trust in the system, they will not adopt the system either. And we find with family doctors and primary care providers, they are as concerned about maintaining the sanctity of their doctor-patient relationship and that privacy as many of the patients we talk to.

Chairman LEAHY. Thank you.

Mr. Chairman, I have other questions, but if I might have your permission, I will submit them for the record.

Senator WHITEHOUSE. Of course, without objection.

Senator KLOBUCHAR.

Senator KLOBUCHAR. Thank you very much, Mr. Chairman.

Dr. Hester, your State of Vermont, like Minnesota, has gone beyond the HIPAA requirements, and as I mentioned, some of the things that Minnesota has included. What do you think would happen if other—we now have sort of a patchwork where some States have gone beyond HIPAA, some have not. People may seek treatment in multiple States. Do you think it would be easier to have this done on the Federal level or to have this done State by State?

Mr. HESTER. I think it is important to have clear Federal standards and guidelines that set the framework, you know, for those policies. For example, the Office of Civil Rights' Framework for Privacy and Security that was issued last December has been a very helpful tool for us. We have suspended the final development of our statewide policies, our operating policies, until we get the clarification on the Federal standards, and we are looking forward to that clarification. It is important.

Senator KLOBUCHAR. And just one side note, Vermont also is a State, like Minnesota, that passed a law prohibiting the sale of patients' pharmacy records.

Mr. HESTER. yes.

Senator KLOBUCHAR. Could you talk a little bit about how this came about? I think patients would be surprised to hear that their pharmacy records were at risk of being sold.

Mr. HESTER. Pharmaceutical companies use histories on prescribing patterns to target physicians for detailing on how to use their products. And so there was concern of that being done in this case without the physician's knowledge or consent as well. So the restrictions have been passed, and they are now being challenged. But it was an issue that was of great concern to the State legislature.

Senator KLOBUCHAR. And this is also included in the House stimulus bill as one of the limitations, the marketing limitation? I think it is.

Mr. HESTER. My understanding, I have not reviewed the details, but my understanding is they are trying to put restrictions in there, yes.

Senator KLOBUCHAR. Okay. Thank you.

Mr. HESTER. We would support that.

Senator KLOBUCHAR. Mr. Houston, Chairman Leahy was going through the other witnesses with some questions, and I saw you nodding your head, maybe the other way, about inclusions of these in the stimulus package. I brought up deliberately this concern of State-by-State regulation. Could you talk a little bit about the limitations proposed and how we can ease the potential burden on providers while trying to get these privacy concerns—which I think we have all agreed are an issue for consumers and we are not going to get the proper use of medical technology if we do not have that kind of confidence.

Mr. HOUSTON. Absolutely. Again, we are all patients, so we all have the same concerns about the protection of our medical information. But I know Deven said it and I have said it, that what we need is a comprehensive framework, and my biggest concern is when I read the privacy and security components of the act, the stimulation package, is what we end up with is a patchwork. And I do not think this patchwork works, in my mind. And there is nothing worse than getting this wrong, because I have seen very directly the impact of trying to inappropriately implement privacy and what the impact potentially can be on patients' care. And so while we all—

Senator KLOBUCHAR. Why is it a patchwork?

Mr. HOUSTON. Well, if you look at the way that—right now there is State preemption even under HIPAA. But when you look at the

act itself, it speaks about RHIOs would be handled one way and other types of organizations would be handled another way, about how they would potentially fit under HIPAA or otherwise have to deal with compliance with certain privacy and security rules.

I just want to get it right and get it right once, make sure that everybody is covered under the same framework. PHRs today are not covered under anything. If you have a personal health record system, you are not covered under HIPAA. Frankly, you might not be covered under anything. And so if we are going to develop an environment which we—and we should be forward-looking because, you know, what we have today and what we are going to have in 10 years or 15 years is going to be dramatically different. And we need to develop a framework which allows us to progress and implement new and novel and progressive health IT, but do it in a fashion where the consumer continues to feel like they are protected, and so that—you know, HIPAA was initially enacted in 1996. I think everybody would agree that it has got a lot of holes. There are a lot of things that, because of the way HIPAA was enacted, really were not covered. We did not think about PHRs. We did not think about a National Health Information Network. And so I just want to make sure we get it right the first time, and I am concerned that we are not here and that we have one bite of the apple, and if we do not get it right, we may find that we are dealing with problems yet again in 2 or 3 or 5 years.

Senator KLOBUCHAR. Ms. McGraw.

Ms. MCGRAW. I think the only place where I would disagree is we just do not think that HIPAA is the right set of protections for the personal health records, in part because HIPAA was designed to allow information to flow among traditional health care entities without necessarily having to ask the patient each and every time. These PHRs are tools that are designed for consumers to have copies of their own records that they can then move, share, they can put their own data in there. That needs to have really a much higher level of consumer control about who can get it and for what purposes. And so while I agree that we need sort of a common framework, a baseline, it has got to also be contextual. Regulation for those products has to target the risks that consumers will face in those products, which are going to be different than when a health care entity holds your data.

My testimony provides a little more detail, but it is a little—it is sort of nuance of difference.

Mr. HOUSTON. And I agree that HIPAA is not necessarily the appropriate vehicle, but we need to be forward-looking and come up with a good framework that really does meet all of our different needs, especially as we see health care IT really transforming.

Senator KLOBUCHAR. Thank you.

Senator WHITEHOUSE. Senator Kaufman.

Senator KAUFMAN. Yes, I want to follow up on that question. I think this economic recovery bill is an incredible opportunity for us to do some things in health care, and the testimony here has been directed toward that. But also it is going to be a lot of money, and it is going to be spent—as Mr. Houston said, if it not spent right, it can cause troubles.

I would really like each one on the panel, if they could, kind of give their opinion on where we are in terms of the present status of the bills, making sure that we are protecting policy at the same time, having much more efficient health IT. Mr. Hester, do you have anything you want to say on that?

Mr. HESTER. The question is the economic stimulus act, the current status of that.

Senator KAUFMAN. Exactly, and the provisions in it for health IT and privacy and where you think we are on that.

Mr. HESTER. I am going to—

Senator KAUFMAN. You can pass.

Mr. HESTER. I can pass? I am going to have to pass.

Senator KAUFMAN. Ms. McGraw.

Ms. MCGRAW. Again, you know, we need a comprehensive framework of protections. HIPAA today does not get us there. What is in the bill takes some concrete steps forward to improving and filling some of the holes. I liked David's "yes, if." I don't have so many "yes, if's," but if all we need to do is address the "if's," then we are pretty close to the goal line. And we should concentrate on doing that rather than having these—you know, wondering whether we can do privacy as part of health IT, because I think we are all pretty much on the same table that you cannot do health IT without privacy.

So we are supportive of those provisions. If there are issues that need to be worked out, we should move forward with doing that as quickly as possible.

Senator KAUFMAN. I take it there are no provisions in the bill that you think are so onerous that they would have to be struck before you would—

Ms. MCGRAW. No, not in my opinion.

Senator KAUFMAN. Ms. Hahn.

Ms. HAHN. I would say that I agree with Deven. I feel that there has been a real willingness on the part of both the House and Senate to work with the e-partnership in terms of addressing our concerns. So we really appreciate moving forward.

Mr. STOKES. Thank you for that question, Senator. Aside from some minor legal clarifications that I have understood from our lawyers that the language might impact non-health-related entities, we see no significant difficulties in adoption of the language as it stands or as it is proposed. But as Dr. Houston pointed out, one of our concerns is providing an ongoing framework or guideline, so this is why my testimony focused on the principles of transparency, control, and security. If we are very clear on what the required principles should be and have ongoing policy discussions as the technology evolves, as medical research evolves, and as the health care ecosystem changes and evolves down the road, we are much better situated to dynamically address those in a basis without coming back again and again for legislative fixes, but are able to have the foundations in the legislation for the regulatory bodies and industries to continue to make progress.

Senator KAUFMAN. Thank you.

Mr. Houston.

Mr. HOUSTON. I think that absolutely I am in support of the health care IT component of the bill. I think health care IT is vital

and we need to move forward with it as fast as we can. I do have serious concerns about the privacy components of the act, though, and I did outline those in my written testimony.

Senator KAUFMAN. Yes, I got those. Yes.

Mr. HOUSTON. And I think there are some serious concerns that I have that could impact providers and their ability to deliver care efficiently. And I also think that, you know, if you read the privacy components of the act, they talk about study and reports and guidelines that need to be established. I really think a lot of that needs to be done up front and then transform that into something that works.

From living in the trenches, I can tell you that you do not want to get things wrong, because you want to improve health care, you do not want to impact health care. And I just see too many things in these provisions that just concern me and are going to get in the way of delivering efficient health care.

Senator KAUFMAN. How long do you think it would take to develop that? I mean, really, we are faced with an economic recovery bill. Clearly, we have economic—I mean, the big reason for doing this is to get the economy moving again.

Mr. HOUSTON. Sure.

Senator KAUFMAN. One of the big emphases is shovel ready, and shovel ready does not just apply to infrastructure. It applies to this. So, you know, if we sit around and study this and come up with a plan—I mean, what do you—I think you have some thoughts.

Mr. HOUSTON. Right. We have done a lot of study. There are a lot of really intelligent people that have great opinions on what we need to do. I think in a year's time, or even less, you could really, I think, put together a comprehensive framework that works.

You know, one of the things about privacy, though, that is different in most everything that is in the stimulus bill is everybody has an opinion in good faith as to what privacy means to them. And it is difficult, often, to bridge the gap between different people's opinions. And none of them are wrong, but we have got to come up with something that works and something that, again, does not impede health care delivery.

Senator KAUFMAN. Thank you. Mr. Chairman, can we let Mr. Merritt, if he has comments?

Senator WHITEHOUSE. Go ahead.

Mr. MERRITT. Thank you. The two areas that I would focus on that I think could be improved, I mentioned one in my oral remarks.

Senator KAUFMAN. Right.

Mr. MERRITT. The issue of de-identified data and health services research. I do not think that there should be the right to opt out of having your de-identified data used for health services research. If you ask anyone who has dealt with large data sets that if you have the ability for selection bias in opting out, you are just not going to have as valid and as reliable research. And I think that as we move forward with comparative effectiveness and evidence-based medicine, we need as much data as possible. And I think you can balance it—again, getting back to my point about balancing. You can balance privacy with progress if you can use de-identified data in that way.

The other point I would mention in the legislation that the House has considered is the impact on disease management or chronic care programs. There are restrictions on reaching out—health plans and health systems, on reaching out to members or patients who might qualify or benefit from these types of programs. And I think that when you are talking about individual health and improving individual health, those data flows and those connection points still need to be protected. I think those can be best suited to be resolved through the rulemaking process at HHS.

And the last thing I will mention that is currently not in the bill, or at least not in the packages that I have seen, is the idea of tying Federal money to certification. When a health system or a provider is going to receive a grant to either purchase a system or an incentive to invest in a system, I think there has to be the tie between the money and certification, and specifically to CCHIT certification, because they do have those protections in place, they do go through a very rigorous process of testing and making sure those products are up to snuff. So I think those four components are very important.

Senator KAUFMAN. Thank you all.

Thank you, Mr. Chairman.

Senator WHITEHOUSE. Thank you, Senator Kaufman.

I would like to start my questions with an observation that comes out of something that Ms. Hahn said when she mentioned that there were—according to, I think it is, a CDC statistics—very close to 100,000 Americans who die every year as a result of hospital-acquired infections. Those of us who have been watching this thing for a while have seen this number move. It began with the IOM report talking about 80,000 American deaths from all avoidable medical errors, and that was only 7 or 8 years ago, as I recall. And then we got to 100,000, and then we got to 100,000 actually just means hospital-based medical errors. And now we have really identified that the field is 100,000 people dying from hospital errors that are the result of hospital-acquired infections.

So the more that we learn about this and the more that we drill into it, the deeper the quality problem and the more astonishing and egregious the consequences for Americans seems to be. I do not think there is anybody in this room or behind this table or listening to this anywhere who has not had the experience of having a loved one in the hospital and have that terrible feeling that you really cannot leave them alone there. Even in the best hospitals, somebody has got to be there to watch out and protect them. And from that to these astonishing consequences, if 100,000 Americans who are being killed every year by anything else, we would be at war. And here we have, I think, an enormous amount of work and investment to make.

So I really applaud all of you for your battle to try to get this right. I think it is really—I opened with my concerns about where this put us politically with respect to the health care reform that we need and what the consequences are of getting it wrong in that larger struggle. But for a lot of humans, this is really a truly human story about someone that they love who they lost, someone in the hospital who they cannot leave alone there. And we just have to do this a lot better.

The discussion, as I have heard it, has focused on having a comprehensive framework, getting it right, being fairly precise so that everybody knows kind of where they stand and what the rules are, and at the same time dealing with the ongoing nature of discovery. I think Mr. Stokes described it as an ecosystem and a dynamic environment. And as we talk about that, we in Congress, people who are legislators, think about different levels at which you can solve a problem. At the very baseline, you can come in, particularly if it is a very static, simple problem, you pass a law, you set the standard, you wash your hands, and you are done with it, and off you can go and worry about something else.

This strikes me as not being that kind of thing. This strikes me as being a highly dynamic environment in which the standard-setting role is less important at a level of detail, if you will, than the architecture-building role. And right now, I do not see in our health care system a good oversight architecture for solving this problem to begin with, and then having somebody or something in place that can continue to adapt to changes through the regulatory environment, continue to correct. To me, this is like landing a plane. You know, you have got to be up, be down. You have got to make adjustments as the wind shifts. You have got to be—that means there has got to be a pilot or a group of pilots, if you will, if it is an organization of some kind. But there has to be some entity that watches this, and I am not comfortable that we have that entity now. As much as I applaud what the CCHIT groups have done and what AHRQ is doing and what—I mean, there are lots of entities that are out there doing it. One of the pieces of advice was do not mess with what is already happening. I think we kind of have to mess with what is already happening because I do not see that we have got the ongoing architecture in place to manage this transformation. I would love all of your thoughts on that point. What should we be—what order of decision should we be making here? Are we talking about actually setting up an organization of some kind that would cope with this? And I know Tom Daschle is going to be our new Director of Health and Human Services. He has written a book about the need for a Federal health board. It seems to me to make a lot of sense that there should be a Federal health board that has some oversight responsibility over protecting privacy and making sure that this gets done.

So that is a long sort of a broad brush of a question, but I would love to hear your responses to it.

Mr. HESTER. I think it is an excellent question and a critical one. At the State level, you know, we have created this organization VITL, which is our health information exchange and has funding, to promote the development of the infrastructure, is putting out the privacy—but its role is education and promotion, and we have been asking whose role is it at the State level to do the oversight, because you do not want the policemen to also be the people who are promoting it. So I agree 100 percent. It is a gap, at least from our perspective at the State level, on how you do this.

The other thing I just want to mention is that you talk about getting it right, and I guess, you know, Garrison Keillor talks about “pretty good,” and I think we want to have a pretty good system, because if you try getting it 100 percent, absolutely zero tolerance

for error, it is not going to happen. And what we have to talk about is the balancing of risk. We have a huge job with the education of our public, the education of our consumers, on there is a huge risk associated with not doing this and what is the balance between an acceptable level of risk on the privacy and security in order to achieve the benefits of reducing the consequences on the delivery system. That is a massive, massive job in terms of getting people comfortable with that balance and that tradeoff.

Ms. MCGRAW. I think notwithstanding the specifics on privacy that are in the bill—and I mention this in my testimony—I think the bill could benefit from a provision that specifically directs the Secretary of HHS—because we do not have this Federal health board that Senator Daschle, soon to be Secretary Daschle, was talking about. But you need to have accountability for putting these privacy and security protections in place, and not just the ones that are regimented in law. But, you know, HIPAA has always been a baseline. You know, States have gone farther; institutions go farther with their policies. Anybody, I think, who gets this significant chunk of Federal dollars should really commit to developing privacy and security policies that are coupled with good technological solutions that make them all work to move forward, not necessarily—you know, we want shovel in the ground, right? So having people submit detailed plans ahead of time is probably not possible to get the impact that we want as soon as we want it. But if you put the Secretary in the position and very specifically task him to hold people accountable, not just for how they spend this money, which they should be, but also what kind of privacy and security protections do you have in place. Do you have protections in place, for example, that meet all of what are common, fair information practices in other contexts? We can do that. I mean, there are plenty of models out there to rely on.

Senator WHITEHOUSE. Ms. Hahn.

Ms. HAHN. I agree there really is not the type of infrastructure in place, and one key part of that public infrastructure is consumer education. Right now, consumers are clueless in terms of when they sign those HIPAA forms. I mean, most people actually think when you sign the form that if you do not sign it, you will not get health care. So, of course, your first thought is: Whatever I need to do to get immediate attention. And in terms of what protections are provided to them, I mean, you see the whole gamut from people feeling that they have a private right of action to sue if the information is made available to feeling that the Federal Government is somehow enforcing it for them.

So whatever we do, we have to make sure that consumers have a clear understanding of what their medical privacy rights are. And in doing so, as we make sure that folks have that understanding, we will remove some of the fear and distrust that we need to move in the direction of more health information technology. So I think that is going to be one key component, and then second is accountability. People need to see—how many people can say here they have seen any entity held accountable for a breach of medical privacy? We only hear about the breaches, but we never find out what is the outcome. And that is going to be critical in moving in that direction.

Senator WHITEHOUSE. Mr. Stokes.

Mr. STOKES. Senator, thank you for that question. I do not think we can wait 1 year or even 1 month or 1 day. As my Vice President testified a week and a half ago in the HELP Committee, we have to start today. We are shipping products today to meet these. We hope that there will be regulations and legislation in a month to help provide more uniform support. We hope that there will be standards and certifications in a year to provide even better support. But we cannot wait and we cannot get it right, perfect. We must start today.

But the focus, we believe, should be on outcomes. If we get too caught up in the processes or the way to get there, we will forget that, just like the researchers and the clinicians in the Mayo Clinic, what we really care about is improving health outcomes and reducing the costs. So all of the policies and the principles should focus on are we getting to those outcomes. What is our return on investment?

And, finally, the privacy principles are outlined about transparency, control, and security. These are actually the same technology principles required by the clinicians and by the researchers to improve quality and reduce cost, because for a clinician I want to be able to have insight into all of the information. I want the transparency as a CIO in a hospital of all the information in my hospital to improve my quality. And I want to be able to control that information so if the FDA sends me an alert, I know within hours or minutes what patients in my hospital system are on those medications, that I do not have to spend days or weeks, like it is today, to track down possible drug interactions.

Thank you.

Senator WHITEHOUSE. Mr. Houston.

Mr. HOUSTON. We clearly need an organization to oversee privacy and security, and I think not from an enforcement perspective but from an oversight. I have said this for a long time, that we are developing this architecture to pass information between entities, across State boundaries, and across the United States. But there really is not an entity in place that provides, I think, the necessary oversight to ensure that appropriate standards are in place, not just for privacy and security but otherwise. And I think we need that. If you look today, we have the Office of Civil Rights that is supposed to enforce privacy. We all want to get this right, but right now there is no infrastructure in place to support trying to get it right.

You know, I do not want to be—I hate to say this. You used the analogy of a pilot and the ups and downs. You want to make sure you are on the right trajectory when you land, and I sure as—you know, just like an airplane is filled with people, you do not want it coming down in the wrong place because a lot of people can get killed. And I think the same thing applies here.

So I think what we need is, again, some type of oversight organization that provides support, almost like an ombuds—I cannot even say the word—ombudsman to do as much support as enforcement.

Senator WHITEHOUSE. Mr. Merritt.

Mr. MERRITT. If I could, I would like to take somewhat of a long view, like 2009 rather than the next 3 weeks. I think the three pil-

lars that you identified earlier are exactly the right ones to focus on: health IT, quality improvement, and payment reform. The one I would like to focus on and urge the Congress to focus on this year is the issue of payment reform, because it can drive the other two. I think it can drive financial incentives for health information technology and the stimulus package actually has that provision and the spirit of that proposal.

Secondly, payment reform can certainly drive quality improvements. We actually held an event at the National Press Club just yesterday, and it answered President Obama's call in his inauguration. He was looking for whatever works. And so we were exploring health care that works. We released a paper that had 60-plus pages of examples of employers and health systems and others who are actually using information technology, best practices, and other programs to improve health, lower costs, drive innovation, and expand access. So I think payment reform can actually be implemented so you can drive others to adopt those best practices.

A Federal health board, while I do not support the outline that Secretary Daschle has put forth in his book, I do think that there is a role for some kind of entity to certify best practices, because there are many companies out there that are using data that can identify best practices, whether it is public or private data. And if there is a body that can actually tie best practices to payment reform, I think it really can be an engine to drive a lot of these innovations.

Senator WHITEHOUSE. Senator Klobuchar.

Senator KLOBUCHAR. Well, thank you very much, Senator Whitehouse.

I had promised Senator Whitehouse I would not talk about Minnesota and the Mayo Clinic until my last round of questioning.

Senator WHITEHOUSE. But then somebody had to say Garrison Keillor, and now there is no holding you back.

Senator KLOBUCHAR. Right. And I would say that Minnesota is a place, to get your quote right, where the women are strong, the men are good-looking, and all the health care providers are above average. So, Dr. Merritt, I wanted to follow up with what you said about the cost, which is very important to me, and the quality. As you know, there has been a study out showing that if all the hospitals in the country followed the protocol that Mayo uses for the last 4 years of a chronically ill patient's life, we could save \$50 billion in Medicare payments over a 4-year period. And some of that has to do with the costs in certain parts of the country, but a lot has to do with the way Mayo is able to standardize their work, how they pay their doctors, but also how they share information and have a team of doctors working together.

So what interests me about what you were talking about is first of all to make sure that in the privacy provisions in the stimulus bill, nothing will stop us in there from going to this overarching framework that we are talking about and, in fact, you intimated that there are some things in there that could help. But I want to make sure that—do you believe that there is anything of these provisions that are—you know, the 3-week provisions we are putting in place that could stop us from going there in terms of making

sure that we can move on to bundled payments and all kinds of things that will create these kinds of incentives?

Mr. MERRITT. I would go back to the two that I identified earlier, which were restrictions on de-identified data, because I know Mayo, just like Inter Mountain, has a very robust research department where they can actually take research from the clinical process, analyze it, and then put it back into the process to identify what—

Senator KLOBUCHAR. Just to make sure, since this is my first day on the Committee, by “de-identified” you mean data that does not have people’s names on it that goes out into the—

Mr. MERRITT. Yes, yes. So if you are working with a data set, it just means that you are dealing with the information, not identifiable information—names, Social Security numbers, et cetera.

So I think that the legislation really does have to be careful with lumping in activities that are used with de-identified data with those that use clearly identifiable data.

Senator KLOBUCHAR. So you want to make sure that any privacy language we have in the stimulus package does not limit the ability of Mayo or other providers in sharing this de-identified data.

Mr. MERRITT. Yes. The reason why we are able to know that Mayo and Inter Mountain and others can provide care that would save Medicare 30 percent is because a team of researchers at Dartmouth has access to Medicare data, and it is de-identified Medicare claims data. And so those kinds of variations they can actually find when they have access to the research and to those data sets. So I think there really has to be careful consideration on provisions that would impact researchers’ ability to do that.

And then, secondly, Mayo and others are very proactive in identifying patients who qualify for various chronic care programs, and they can focus on wellness before it becomes disease.

Senator KLOBUCHAR. This is what you talked about earlier with being able to reach in and get the patients that you think need the help.

Mr. MERRITT. Correct. And many of these fall under the current definition of health care operations. Some of the language I think could actually harm a health system’s ability, whether it is a system like UPMC or Mayo or a health plan, to have the ability to actually connect with a patient and say we have looked at your record, we understand that you have X, Y, and Z, we think you are in danger of, you know, Type 2 diabetes, or you need to control your obesity, or whatever the condition may be. If there are restrictions on the system or the entity reaching out to that consumer or patient, again, I think you have to be very careful because you want—at the end of the day, we all want the patient to get the care that they need. But if there are privacy restrictions that do not allow the connection and the education, I think that could ultimately harm individual health.

Senator KLOBUCHAR. So are you concerned there is language in there right now that could do that?

Mr. MERRITT. Yes.

Senator KLOBUCHAR. Limit it.

Mr. MERRITT. Yes.

Senator KLOBUCHAR. All right. Well, we will have to look at that, because I have found it very helpful. I know it is helpful for Mayo and these other groups that have done so well to be able to have that research. I also think in the end it would be nice if it was done the right way, with no security breaches and everything we have talked about, to be able to have that data on a national basis so we can get the right protocols in place, because there clearly has been a problem with decisions being made with the lack of research.

Thank you.

Senator WHITEHOUSE. Before we proceed, just one piece of administrative housekeeping. Letters from the Vermont Information Technology Leaders, from the Coalition for Patient Privacy, and from the American Civil Liberties Union will be added to the record of this hearing, without objection.

One of the things that I come across pretty frequently—but I have not really been able to source it so I will float it out to the expert panel and see if you have any information on this—is that when people have chronic or multiple illnesses and they have a lot of exposure to the health care system, their appetite for electronic health records is very high, and their tolerance for privacy concerns is also quite high because they are living in the environment where they can see the value of the electronic health record in the communication and the privacy concerns just do not matter as much to them when they are ill.

I see heads nodding. Is that anybody's experience out there? And might it be helpful to focus initially in terms of trying to develop some of this, particularly for going forward in a dynamic environment, on those very high expense, very high contact either chronic or multiple illness patients in the system?

Mr. Merritt.

Mr. MERRITT. If I may, one thing the Federal Government could actually do to address that problem is through providing information for Medicare beneficiaries based on information that CMS actually has. For instance, we have talked a little bit about personal health records—Microsoft, there are private companies, there are private payers that have been in this space for a long time. CMS has a very small pilot in South Carolina, and they just announced two others in Arizona and Utah. But what I would propose is that the Federal Government, through CMS, actually put up a consumer portal so that any beneficiary who wants to can actually log on and see just a snippet of their information. And if they want to share that with their doctor, I think that would be incredibly valuable.

Some studies say that the average beneficiary is on six medications. That is the average. And the average beneficiary sees 13 different doctors throughout the course of a year, and there is no coordination between them. So having patient-controlled access to that information I think would be incredibly valuable, and I would certainly open it up for other comments as well.

Senator WHITEHOUSE. Mr. Houston.

Mr. HOUSTON. I would agree with the proposition that people that have chronic illnesses absolutely will be more interested in having PHRs, and I think the insurance companies would likely

also want to manage that population much more aggressively to try to reduce inpatient admissions and improve quality of care, things of that sort. But I do not believe that those people believe that their privacy is less important because probably one of the primary types of chronic illness in the United States is behavioral health illnesses, depression and other things, and I think those people could definitely be helped by having a PHR. But they are also a population that is probably more concerned about the privacy of their information.

So I think privacy has to be done well throughout regardless of what the population is, regardless of what the—

Senator WHITEHOUSE. Yes, I could not agree with you more about that. My point was that if you are looking for early adopters who see the real value of this, there seems to be a kind of fortunate correlation between the people for whom this would be the most helpful and their willingness in turn—

Mr. HOUSTON. Absolutely.

Senator WHITEHOUSE [continuing]. To try to achieve that value in their own health care.

Mr. HOUSTON. Take diabetes alone. I think that that is probably a chronic illness for which having good tools for patients would clearly benefit patients and reduce costs and improve quality of life. I mean, I think that is a clear winner. And you are right, those people are very concerned about trying to manage their condition.

Senator WHITEHOUSE. Dr. Hester.

Mr. HESTER. You are right on target. One of the main themes of health care reform in the State of Vermont has been focusing on patients with chronic illness. We have sustained attention on that. Again, I mentioned in my testimony we have pilots, enhanced pilots in three communities which involve payment reform, the creation of community care teams, and the provision of information technology tools for the practices and for the patients that will cover 10 percent of the Vermont population by the end of this quarter.

It is not just a matter of the benefit to the patients. You cannot do chronic illness care, best practice, you cannot be proactive in reaching out to patients, to a diabetic who has not had their hemoglobin A1c in the last 6 months unless you have those tools in place and the patients understand it.

So from the standpoint of—Ed Wagner has developed something called the “Chronic Care Model,” which is sort of his approach to saying how do you do best practice. It involves the combination of a proactive care team of providers and engaged patients. You know, the information technology is critical to supporting both the care team and patient engagement, and we have found it to be a very rich area of collaboration and one reason that we focused—one of VITL’s major pilot programs has been in providing those information tools, supporting those information tools in those pilot communities. So I would be happy to provide you with some additional information if you are interested.

Senator WHITEHOUSE. Thank you. I would appreciate that.

Mr. Stokes.

Mr. STOKES. Senator, I agree that this is a critical area and a very opportune area for cost savings and improving quality. But as

I pointed out before, there is no need to wait. We have a cooperation with Cleveland Clinic today that pilots and targets the chronic care disease population within the Cleveland Clinic through a combination of different doctors and specialties within the clinic and the chronic patients at home, because we have found that if they are in a remote setting, they will take their blood glucose measurements more often. There is better compliance and better participation all through HealthVault without having to sacrifice any patient privacies, maintaining the transparency and control.

So as was discussed, if we can move forward and have better foundations and better infrastructure and better guidance over time, that would be great. But even today, we are focusing on the outcomes to move this forward.

Senator WHITEHOUSE. Dr. Hester again?

Mr. HESTER. Just one more comment. The success of that Chronic Care Model is completely dependent upon payment reform, as being discussed earlier, and there is a regional collaborative being formed in the New England States, including Rhode Island—it is being sponsored by the Milbank Fund—to have a regional demonstration in patient-centered medical home and to try to provide a vehicle for Medicare to participate and support. What we are finding is the States are further ahead in terms of multipayer payment reform involving commercial insurers and Medicaid, but we are having difficulty getting Medicare to the table, and it is something we could use some assistance in the new administration to move forward, and we are hoping this regional collaborative will be a vehicle.

Senator WHITEHOUSE. Well, I think I will take this opportunity to bring the hearing to a close. I want to thank all of you very much for your testimony and for your work in this area. I will just re-emphasize what I said at the beginning. I think we are headed—remember when the Clinton administration tried health care reform and they got Harry and Louise'd, and that put an end to that particular effort.

Senator KLOBUCHAR. But, Mr. Chair, now Harry and Louise are on Medicare Part D, and now they support the effort.

[Laughter.]

Senator WHITEHOUSE. And I think now the model is no longer Harry and Louise. Now the model is Thelma and Louise, and we are all in the car, and the cliff is right in front of us. And if we do not get this solved through technology, through systems reform, through better quality care, through a more rational payment system, then we will get to the edge of that cliff. And when we are there and we have to go into the other toolbox and throw people off of health coverage and thin out our already tragically thin benefits and put even more costs on our business community, which is already laboring uncompetitively under health care costs compared to their foreign competition, and tell providers who are already cross-subsidizing in order to stay in the Federal health care system that we are going to pay them even less—it is going to be a nightmare.

And so you work to guide us through the privacy hazard to solving these problems the good way I think is really at the absolute apex of issues that our country faces. And I applaud you for it. I

urge you to be as persistent and energetic as you can, and I think you have seen from the turnout in this Committee and from how long people stayed that this is a matter that has great interest, and we truly look forward to working with you.

The record of the Committee will stay open for an additional week in the event that anybody has anything they would care to add, and without anything else, I appreciate again that you have all come in here. I appreciate everybody's attention, and the hearing is adjourned.

[Whereupon, at 11:14 a.m., the Committee was adjourned.]

[Questions and answers and submissions for the record follow.]

QUESTIONS AND ANSWERS

Health IT: Protecting Americans' Privacy in the Digital Age

**Witness Questions from The Honorable Patrick Leahy, Chairman,
Senate Committee on Judiciary**

Questions for Ms. Hahn

1. A recent survey shows that the majority of consumers are unaware of laws that protect the privacy and security of personal health information. According to the California Healthcare Foundation, despite Federal protections, a majority of consumers remain concerned about the privacy of their personal health information and are largely unaware of their rights. You are an advocate for one of the Nation's leading consumer protection organizations. Are you concerned that consumers are unaware of their federally mandated privacy rights.

Consumers Union is concerned that consumers are unaware of their federally mandated privacy rights. We recognize that consumers struggle with a lack of understanding about their rights provided under existing medical privacy protections. For example, a national consumer health privacy survey illustrated the confusion that exists.¹ In this survey, two-thirds of the survey respondents stated that they were aware of federal protections for their personal medical records, and 59 percent recall receiving a privacy notice but only 27 percent believe they have more rights than they had before receiving the notice.² Simply put, the growing evidence of confusion must commit us to better educating the public, not to undermining support for the medical privacy protections for which the public clamored for decades.³ In keeping with this effort to better inform the public, Consumers Union has used our publication *Consumer Reports* to inform our 8 million subscribers about their rights, as well as encourage others to visit the Health Privacy Project website which has merged with Center for Democracy and Technology to download their user-friendly brochure "Know Your Rights."

When consumers are confused, they are fearful that there is widespread misuse of personal medical information. This concern regarding the privacy of their medical information manifests itself in consumers engaging in "off the grid" medical care. These privacy-protective behaviors include patients providing false or incomplete information to physicians, doctors inaccurately coding files or leaving certain things out of a patient's record, people paying out of pocket to avoid a claim being submitted, or in the worst cases, people avoiding care altogether.⁴ Therefore, it is critical that consumers have a full understanding of their medical privacy rights and confidence in the federal health privacy law to preserve the confidentiality of their medical records. Otherwise, people are forced to choose between shielding themselves from discrimination and receiving health care services.

According to a California Healthcare Foundation survey, the majority of Americans who are least likely to receive notification of their privacy rights are minorities. At the hearing, you testified that barriers affecting consumers' access to notification about their health privacy rights may disproportionality impact minority communities. What steps should Congress take to ensure that all consumers, including minority consumers, are better educated about their health privacy rights?

¹ California HealthCare Foundation, "National Consumer Health Privacy Survey", November 2005.

² Ibid.

³ Ibid.

⁴ Ibid.

It is true that the California Healthcare Foundation Survey found that consumers remain concerned about the privacy of their personal health information. Sixty-seven percent (67) of respondents to this survey reported that they are "somewhat" or "very concerned" about the privacy of their personal medical record, as opposed to seventy-three (73) percent of racial and ethnic minorities.⁵ To address the concerns of racial and ethnic minorities regarding the privacy and security protections related to health IT, it will require an aggressive public education campaign that separates myths from facts about the new privacy protections contained in the American Recovery and Reinvestment Act of 2009.⁶ This campaign effort needs to be a public and private partnerships that includes the U.S. Department of Health and Human Services working in collaboration with community based organizations such as the National Council of La Raza, National Association for the Advancement of Colored People (NAACP), National Urban League, National Congress of American Indians, Asian and Pacific Islander American Health Forum and other key organizations from the racial and ethnic minority communities that can assist with disseminating information regarding health privacy rights.

Witness Questions from The Honorable Arlen Specter

Questions for Ms. McGraw, Dr. Hester and Ms. Hahn

1. Do you believe the privacy provisions that are part of the Health IT legislation that has been inserted into an appropriations bill through a closed-door process would benefit from going through regular order as is required of most Senate legislation?

Consumers Union along with members of the Consumer Partnership for e-Health, a non-partisan group of consumer, labor, patient, and research organizations is dedicated to broadening access to health care, and improving the quality of care by ensuring that consumer's medical information is safeguarded in the health care arena. The Center for Democracy and Technology is a member of the Consumer Partnership for e-Health as well and we echo their response below.

"Congress is proposing to spend \$20 billion to promote health information technology (Health IT) adoption and implementation as part of the economic recovery legislation. Health IT holds enormous potential to improve patient care and the efficiency of our health care system. Survey data shows that the American public supports health IT. At the same time, the public is very concerned about the risks that health IT poses to privacy. Building public trust in health IT systems is critical to reaping the technology's benefits.

We need a comprehensive framework of privacy and security protections to build public trust in health IT. A commitment to spending significant federal dollars to advance health IT must be coupled with a strong commitment to privacy and security. As a result, it is critical that privacy provisions be part of any legislation that promotes the adoption of health IT.

The urgent need to ensure that the public's health information remains private and secure in e-health systems justifies the inclusion of privacy provisions in the economic recovery legislation." Having said that, like most legislation, refining amendments are often needed, and we hope you will conduct rigorous

⁵ California Healthcare Foundation, National Consumer Health Privacy Survey 2005, p. 1.

⁶ Janlori Goldmam, Director Health Privacy Project, before the National Committee on Vital and Health Statistics regarding the HIPAA privacy regulation: implementation, compliance, and impact on health care, November 19, 2003.

oversight of the implementation of the new law to detect early problems and make necessary corrections.

2. What steps can be taken to improve patients' knowledge of their rights under existing federal legislation?

Consumers Union along with members of the Consumer Partnership for e-Health, a non-partisan group of consumer, labor, patient, and research organizations is dedicated to broadening access to health care, and improving the quality of care by ensuring that consumer's medical information is safeguarded in the health care arena. The Center for Democracy and Technology is a member of the Consumer Partnership for e-health as well and we echo their response below.

"Under the current Privacy Rule, each covered entity, with certain exceptions, must provide a notice of its privacy practices, including patients' rights under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. However, more often than not, privacy notices are written in language that the average person cannot understand. Further, rarely do patients focus on the details of such notices, and many wrongly assume that the existence of a "privacy policy" means that their health information will not be shared, even when the policy and the accompanying consent form say just the opposite.

Thus, while the privacy notice required under HIPAA is an important tool for informing patients of their rights, there is more that can be done to improve patients' knowledge of their rights. The economic recovery bill takes a step forward by authorizing funds for the Department of Health and Human Services to educate both patients and their health care providers on their rights and responsibilities under HIPAA. The Obama Administration could go further and disseminate a model privacy notice to be used by entities covered by HIPAA. The Administration could also impose (or encourage) a "layered" notice approach, where patients are provided with a one-page, easy-to-read summary of the most critical of the Privacy Rule's provisions; entities must then make a longer, more detailed notice available for patients who have further questions or who need more information."

3. Do you believe that consumers are or will be properly aware of the steps taken to secure their electronic health records? In your view, would consumers be more comfortable with the adoption of health IT if their providers were required to describe the steps taken to secure electronic medical data, including, for example, the encryption of records and maintenance of access logs?

Consumers Union along with members of the Consumer Partnership for e-Health, a non-partisan group of consumer, labor, patient, and research organizations is dedicated to broadening access to health care, and improving the quality of care by ensuring that consumer's medical information is safeguarded in the health care arena.

"No, I do not believe that many consumers are aware of the steps that entities take to secure their electronic health records. All entities covered by HIPAA are required to adopt security protections, but the law does not require that consumers be provided with detailed information on an entity's security practices. (We assume that some entities do voluntarily provide information on security practices to consumers to demonstrate their strong commitment to security – but to the best of my knowledge, there has been no systematic study of this or the impact that it has on building consumer trust and adoption.)

We believe it would increase consumer trust if security requirements were strengthened beyond drafts of the economic stimulus package and if consumers knew more about the security practices of entities that maintain or have access to their health data. But good security practices are not sufficient on their own to build public trust. We also need a comprehensive framework of privacy policies that clearly set forth who can access health information and for what limited purposes, and that are more aggressively enforced. Robust security practices will do little to build public trust if our privacy policies and practices permit overly broad access to the data."

Witness Questions from The Honorable Orrin G. Hatch
Questions for all panel members:

I strongly support health IT, but believe this must be done very carefully so that we give health care providers the proper incentives to adopt technology without increasing regulatory burdens and costs.

Many health care groups have expressed concerns that requiring new and untested privacy mandates could damage the ability of providers to communicate with patients about treatment options and alternatives.

They are also concerned that additional privacy requirements would add costs to the health care system, and actually discourage providers from adopting the very health IT we want them to use.

Do you share these concerns and how would you recommend Congress and the Administration prevent these problems from occurring?

Consumers Union along with members of the Consumer Partnership for e-Health, a non-partisan group of consumer, labor, patient, and research organizations is dedicated to broadening access to health care, and improving the quality of care by ensuring that consumer's medical information is safeguarded in the health care arena.

"Ensuring appropriate privacy and security protections for electronic health information may require covered entities to adopt stronger policies and practices. Such entities will also need to update their care delivery and business models in order to ensure we reap the full benefits of transitioning health care to the digital age. These changes will not occur without some effort by industry, and we applaud providing federal financial support to the health care sector (particularly for primary care practices and safety net hospitals and delivery systems) to help us achieve a better, more interconnected health care system.

CDT believes the privacy provisions in the economic recovery package take workable, concrete steps toward the realization of a comprehensive framework of privacy protections that builds trust in health IT. These provisions build on the HIPAA Privacy and Security rules, a regulatory environment that is familiar to the health care industry, and do not impose a new and unfamiliar privacy infrastructure. The provisions in the bill also were carefully crafted to avoid imposing burdens on the health care industry that outweigh their benefits. Further, in circumstances where new functionalities are required to be adopted, the Secretary is tasked with developing regulations that further detail the requirements on industry, and he or she must take into account the administrative and cost burdens on industry, as well as the potential impact on health care, in the development of these regulations.

As health IT is more widely disseminated, it will be critical for Congress and the Administration to continue to monitor developments to ensure that health IT is being effectively deployed to improve health care, and that adequate and workable privacy and security protections remain in place."

Witness Questions from The Honorable Orrin G. Hatch
Questions for all panel members:

While I support a strong commitment to patient privacy, I am worried that some of the proposals under consideration would have unintended consequences for patients, physicians, and hospitals.

Specifically, I am particularly concerned about a proposal that would *prohibit* the use or disclosure of protected health information for routine health care activities without individual consent.

What are your thoughts on this type of proposal?

Any thoughts on how a prior consent requirement would affect patient care, quality improvement and research?

Consumers Union along with members of the Consumer Partnership for e-Health, a non-partisan group of consumer, labor, patient, and research organizations is dedicated to broadening access to health care, and improving the quality of care by ensuring that consumer's medical information is safeguarded in the health care arena. The Center for Democracy and Technology is a member of the Consumer Partnership for e-health as well and we echo their response below.

"Patient consent for every routine use of health care information provides very weak protection for privacy, unnecessarily burdens patients, and creates obstacles to the sharing of information within the health care system for important health care purposes. CDT does not support an approach to privacy that relies too much on patient consent, and there is no such provision in the economic recovery legislation.

Although patient consent is not a panacea, it is one component of a comprehensive framework of privacy and security provisions that should govern the sharing of health information. We believe health information should be allowed to flow without requiring patient consent for core health purposes, including treatment, payment, and those limited administrative functions that are critical to care delivery and payment. At the same time, health IT enables us to provide consumers with opportunities to make more meaningful choices about the use of their health data. As a result, we need a strong role for patient consent with respect to access and disclosure of information in personal health records. Patients should also have choices with respect to whether or not their health records are part of a state, regional or national health information exchange. We also need to ensure that where patient consent is required, our health IT systems have the capacity to honor that consent.

With respect to the use of patient information for health care quality activities, we share your concerns about requiring consent or authorization for the use of this information, particularly when the quality assessment and improvement activities take place within an institution or an organized and integrated delivery system. However, we also believe that it is not necessary to use fully identifiable patient data for quality assessment and improvement functions, and that entities conducting such activities should be able to accomplish their purposes using data that has been anonymized or masked, which provides greater protection for privacy.

With respect to research, the HIPAA Privacy Rule permits a covered entity to use and disclose protected health information for research purposes in certain circumstances without a patient's consent, where the risks to privacy are minimal. The economic recovery legislation does nothing to alter these research rules (although early drafts do limit the remuneration received for such research to the costs associated with gathering and transmitting the data). A covered entity may disclose health information without patient consent to researchers if the researcher: (1) has obtained authorization from an Institutional Review Board or Privacy Board to proceed without consent; or (2) represents to the covered entity that he or she is seeking

health information solely to prepare a research protocol or to conduct an activity preparatory to the main research (and he/she does not remove the health information from the premises); or (3) represents that he or she is seeking only the health information of someone who is deceased and the information is necessary for the research. Covered entities may also use or disclose, without an individuals' authorization, a limited data set of information for research purposes. Limited data sets are data that has been stripped of common patient identifiers, which greatly reduces the risks to privacy."

Witness Questions from The Honorable Orrin G. Hatch **Questions for all panel members:**

Throughout all of your testimonies you all agreed that it is essential that there be privacy protections in place as we move nationally toward health IT. But, it seems that most of the ideas discussed were rather broad.

Do you have any specific suggestions as to what privacy protections should be considered?

Consumers Union along with members of the Consumer Partnership for e-Health, a non-partisan group of consumer, labor, patient, and research organizations is dedicated to broadening access to health care, and improving the quality of care by ensuring that consumer's medical information is safeguarded in the health care arena. The Center for Democracy and Technology is a member of the Consumer Partnership for e-health as well and we echo their response below.

"Privacy Solutions That Enable Health IT

- Ensure that all entities that collect, store or manage personal health information are required to comply with baseline health information privacy and security protections:
 - Adopt a broad policy framework based on fair information practices that governs all federal efforts to advance health IT.
 - Ensure that traditional health system entities who are covered by HIPAA and entities that handle personal health information on their behalf ("business associates") are at least held accountable to the minimum privacy and security standards in the HIPAA rules.
 - Ensure that health information exchanges (commonly known as HIEs or Regional Health Information Organizations (RHIOs)), which today are not covered under HIPAA, are required to comply with HIPAA requirements, either as covered entities or business associates depending on their structure and functions.
 - Establish privacy and security protections for personal health information stored with or managed by non-health care entities (such as employers and Internet companies). It is neither sufficient nor effective to extend the HIPAA Rule to these entities. Instead, Congress will probably have to pass a statute with some parameters and authorize the FTC, in consultation with HHS, to develop and enforce appropriate protections.
- Establish a federal, individual right to be notified in the event of a breach of identifiable health information; such a requirement should probably include an exemption for information that is encrypted.

- Ensure appropriate standards are in place for the use of data that has been stripped of identifiers so that it is anonymous to the data holder. Includes revisiting the current standards in the Privacy Rule for de-identification and use of what are called "limited data sets" to ensure they continue to minimize the risk of re-identification while serving the needs of researchers --- and others, and establishing penalties for re-identification that apply to all data recipients.
- Establish clear rules regarding the use of personal health information for marketing and commercial purposes that are not solely reliant on patient authorization. Include tightening the definition of marketing in the Privacy Rule for HIPAA covered entities, as well as setting clear standards for the use of data for marketing and other commercial purposes by non-health care entities.
- Ensure strong oversight and accountability for all entities handling health information. Will require strengthening HIPAA enforcement by: (1) clarifying the HIPAA statute so that criminal penalties can be imposed against individuals, and to ensure civil monetary penalties are imposed in cases of willful neglect of the rules; and (2) providing additional enforcement resources, such as through an increase in appropriations to HHS and/or by expressly authorizing states to enforce privacy protections. Will also require FTC to take a more active role to ensure enforcement of consumer protections against non-health care entities.
- Revisit the scope of the concept of "health care operations," a category of uses under the current Rule that does not require patient authorization. Reconsideration of the scope of the exception is particularly appropriate for situations where data is shared outside of a HIPAA-covered health care entity for such purposes as research. Require the use of anonymized data for health care operations that do not need identifiable data. Consider whether some purposes under "operations" should require patient authorization.
- Strengthen the role of patient consent by requiring opt-in before patient health information is stored in or shared through an electronic health information exchange, particularly where the exchanges are used for purposes beyond treatment (requires legislation), and by ensuring that health information stored in personal health records and other consumer-facing tools is accessible only with patient authorization (may require legislation or enhancing current legal authorities). Consider also strengthening the HIPAA "right to restrict" the access and disclosure of health information, particularly for more sensitive health data.
- Ensure individuals can promptly obtain electronic copies of their health information from health care providers and plans and require entities with electronic health record systems to provide audit trails of uses and disclosures to individuals upon request.
- Devote more resources to education about health privacy and the protections under current law, for both patients and for those required to comply with the laws, and develop and disseminate model privacy notices (a one-page summary notice and a longer, more detailed notice) that more clearly explain how information can be used and disclosed and patient's rights under current law."

Witness Questions from The Honorable Orrin G. Hatch
Questions for all panel members:

Greater adoption of health IT has been recognized as enabling improved chronic disease management through better coordination of care. In order to coordinate care, providers need to be able to have access to patient data collected via health IT.

For example, a provider could generate a list of all diabetic patients in a practice to ensure screening tests are up-to-date, prescriptions are filled, or to determine if any patients are overdue for a visit.

What impact could privacy restrictions have on this and other care coordination functions?

Consumers Union along with members of the Consumer Partnership for e-Health, a non-partisan group of consumer, labor, patient, and research organizations is dedicated to broadening access to health care, and improving the quality of care by ensuring that consumer's medical information is safeguarded in the health care arena. The Center for Democracy and Technology is a member of the Consumer Partnership for e-health as well and we echo their response below.

"Currently, there is nothing in the bill's provisions that would hamper a provider's access to health information for these purposes. Many of these, when done by a provider, would be considered part of treatment – and the bill does not change the ability to use information for treatment purposes.

To the extent that these activities are considered health care operations under HIPAA, the bill tasks the Secretary with reviewing the scope of the category of health care operations, and CDT supports a thorough review. Currently, the category is entirely too broad, particularly with respect to the sharing of identifiable data for operations purposes outside of a HIPAA-covered health care entity (see footnote below for a complete list of the activities within health care operations).⁷ Under HIPAA regulations today, fully identifiable data can be used for any health care operation, and many of the activities in operations could be done with anonymized data (allowing the entity to get what it needs from the data but also providing greater protections for patient privacy). There may also be some components of operations that should require patient authorization. Giving the Secretary the full discretion to review this category as part of a regulatory process, which allows all stakeholders to weigh in with any concerns, is the appropriate way to address this issue."

⁷ Health care operations include: (1) Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination; (2) Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities; (3) Underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims; (4) Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs; (5) Business Planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and (6) Business management and general administrative activities, including those related implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity. 45 C.F.R. §164.501.

Witness Questions from The Honorable Orrin G. Hatch
Questions for all panel members:

I have heard concerns expressed that by putting very narrow privacy constraints on the use of health information – like allowing specific information to be hidden and permitting medical treatment paid out-of-pocket to be kept secret – you encourage greater fraud and abuse, increase the incident of improper payments, and double-billing, among other things.

What is your take or reaction to those concerns and what solutions, if any, would you propose?

Consumers Union along with members of the Consumer Partnership for e-Health, a non-partisan group of consumer, labor, patient, and research organizations is dedicated to broadening access to health care, and improving the quality of care by ensuring that consumer's medical information is safeguarded in the health care arena. The Center for Democracy and Technology is a member of the Consumer Partnership for e-health as well and we echo their response below.

“Under the current Privacy Rule, patients have the right to request a restriction on uses and disclosures of their personal health information for treatment, payment, and health care operations. However, a covered entity is under no obligation to grant the request. Therefore, though patients have a right to restrict, this right is not very meaningful.

In cases where a patient wants to pay for health care out-of-pocket, CDT believes a covered entity should honor a request not to disclose information related to that care to an insurer specifically for payment purposes. By failing to honor a patient's request to restrict, a covered entity sending a claim for a service that had been paid in full would not only be committing fraud; it would also be violating the HIPAA Privacy Rule.

Electronic systems, which have greater tracking and segmentation abilities, can help entities better comply with these restrictions in the limited instances when they are requested and can help auditors detect fraud and double billing. Most people with insurance want their care to be paid for by the insurer; only those with heightened privacy concerns, or who are seeking sensitive care (such as mental health or substance abuse) as well as trying to hide a particular condition will seek to take advantage of this.”

Senate Committee on the Judiciary
Hearing on "Health IT: Protecting American's Privacy in the Digital Age"
January 27, 2009

Response to written questions by Jim Hester

1. Senator Hatch re Vermont's estimated savings by converting to electronic files.

Ans: As part of the state legislature's review of the proposed state Health IT fund, staff were asked to estimate these savings. We calculated the Vermont savings based on the working papers supplied by the Commonwealth Fund which were used to develop their estimates of the ten year impact of a similar national IT program that was published in the report "Bending the Curve" in December 2007. We projected total 10 year savings in Vermont to be \$320 million for an IT investment of \$31 million. Savings exceeded costs after four years.

2. Senator Leahy re 'best practices' to achieve balanced privacy protection for electronic health records

Ans: As a former national Baldrige award examiner, I am careful about making sure that 'best practices' are based on sound evidence. Unfortunately, the field of health information exchange is new enough that we do not have sufficient experience to establish best practice as yet, particularly in establishing the balance point that I spoke of in my testimony. Based on my experiences in participating in this debate in Vermont I personally support a policy which includes

- a positive opt in by each patient to participate in the exchange
- a periodic (every two years) reminder to the patient of their ability to opt out, if they wish
- if the patient has opted in, no requirement for a second confirmation of consent when sharing information for specific authorized purposes. The exception to this is specific class of information which by statute requires secondary consent. (See the chart in my written testimony.)
- the right of the patient to access their data and correct errors
- the right of the patient to request a listing of how their personal data has been shared with other providers or covered entities.

3. Senator Hatch re specific suggestions for privacy protections

Ans: See response to question #2

John Houston's Responses
To the
Questions of the Honorable Orrin G. Hatch
U.S. Senate Judiciary Committee
Health IT: Protecting Americans' Privacy in the Digital Age January 27, 2009

Panel Question 1: *I strongly support health IT, but believe this must be done very carefully so that we give health care providers the proper incentives to adopt technology without increasing regulatory burdens and costs.*

Many health care groups have expressed concerns that requiring new and untested privacy mandates could damage the ability of providers to communicate with patients about treatment options and alternatives.

They are also concerned that additional privacy requirements would add costs to the health care system, and actually discourage providers from adopting the very health IT we want them to use.

Do you share these concerns and how would you recommend Congress and the Administration prevent these problems from occurring?

Response: We too strongly support Health IT and encourage its inclusion in the stimulus bill.

While we do not believe that the imposition of additional privacy regulations will discourage providers from adopting Health IT, we do believe that the imposition of the wrong privacy regulations will establish barriers that are contrary to the purpose of adopting Health IT.

The Latin phrase "primum non nocere" is commonly translated as "first, do no harm". These untested privacy mandates could impede the efficient and effective delivery of health care, and could very well result in harm and increase costs.

It appears that the proposed privacy regulations further a patchwork of disparate privacy regulations, rather than establishing a comprehensive framework that will support the adoption of Health IT, and the development of a nationwide health information network.

We believe that a reasoned and methodical approach should be employed to establish a common federal framework that holistically addresses the privacy of health information. This would apply to all entities that handle health information (including PHR providers, Health Information Exchanges (HIEs), Regional Health Information Organizations (RHIOs) and other entities that had historically fallen outside the coverage of HIPAA), regardless of whether the entity is covered by HIPAA. This framework should replace HIPAA and existing state laws.

I would stress that the creation of a common federal framework must be carefully and thoughtfully developed to maintain the balance between patient privacy and access to information essential to the patients' care. I would suggest that HIPAA be used as the foundation for this framework.

Panel Question 2: *While I support a strong commitment to patient privacy, I am worried that some of the proposals under consideration would have unintended consequences for patients, physicians, and hospitals.*

Specifically, I am particularly concerned about a proposal that would prohibit the use or disclosure of protected health information for routine health care activities without individual consent.

What are your thoughts on this type of proposal?

Response: This type of proposal would impede access to important information and would likely result in patient harm and a decrease in the efficiency of health care delivery.

Any thoughts on how a prior consent requirement would affect patient care, quality improvement and research?

Response: A prior consent requirement would impede access that is important for providing effective and efficient delivery of health care. Additionally, a prior consent requirement will make retrospective quality improvement activities more difficult to perform. Further, a well established consent/approval process already exists for research. Additional consent requirements will interfere with the ability of researchers to perform important research, and to recruit research subjects.

I believe that HIPAA appropriately balances the instances where consent is required against the need for timely patient care information. As such, I do not believe that additional consent requirements should be included. Rather, HIPAA should be used as a model for consents, when establishing a common federal framework.

Panel Question 3: *Throughout all of your testimonies you all agreed that it is essential that there be privacy protections in place as we move nationally toward health IT. But, it seems that most of the ideas discussed were rather broad.*

Do you have any specific suggestions as to what privacy protections should be considered?

Response: As discussed above, I believe that a reasoned and methodical approach should be employed, to establish a common federal framework that holistically addresses the privacy of health information.

Panel Question 4: *Greater adoption of health IT has been recognized as enabling improved chronic disease management through better coordination of care.*

In order to coordinate care, providers need to be able to have access to patient data collected via health IT.

For example, a provider could generate a list of all diabetic patients in a practice to ensure screening tests are up-to-date, prescriptions are filled, or to determine if any patients are overdue for a visit.

What impact could privacy restrictions have on this and other care coordination functions?

Response: Access to health information is vital for the effective and efficient treatment of both chronic and acute illness. Under HIPAA, access to health information does not require a patient's consent. This is one of the basic principles that must be carried forward from HIPAA.

Panel Question 5: *I have heard concerns expressed that by putting very narrow privacy constraints on the use of health information – like allowing specific information to be hidden and permitting medical treatment paid out-of-pocket to be kept secret – you encourage greater fraud and abuse, increase the incident of improper payments, and double-billing, among other things.*

What is your take or reaction to those concerns and what solutions, if any, would you propose?

Response: I cannot say whether allowing information to be hidden will increase the likelihood of fraud and abuse. However, withholding information interferes with the effective

and efficient delivery of healthcare. While a patient may either not desire to disclose information, or not recognize the importance of disclosing information, such information may be vital for the treatment of the patient.

For example, consider a patient who is being treated for a psychiatric illness and has been prescribed certain medications. If the medication is not contained in the patient's record, and the patient is brought to a hospital's emergency department in an unconscious state, an emergency department physician could prescribe other medications that may cause a serious and potentially devastating adverse reaction.

Houston Question 1: *Mr. Houston, you mentioned in your testimony that the establishment of specific standards may actually retard or prevent the adoption of appropriate security measures, especially in light of emerging technologies.*

Do you support a baseline standard for security precautions?

Response: I do not believe that specific technology standards should be established. Security requirements may vary dramatically among organizations, due to the organization's size and the manner in which it utilizes information technology and also the stage of its information technology implementation. Creating specific standards without the funding for the necessary IT investment would place an unreasonable burden on many organizations. Additionally, security technologies and threats can change rapidly. As a result, setting technology standards may impede organizations ability to employ appropriate security.

I believe that the current HIPAA security rule does a reasonable job of setting security standards in a technology neutral manner.

Houston Question 2: *Mr. Houston, you stated that privacy restrictions will be difficult, if not impossible, to administer and moreover, could deprive caregivers of vital information necessary to treat the patient appropriately.*

What makes these restrictions so difficult?

Are there no inexpensive alternatives?

Response: My comments were in response to the proposal to restrict access by health plans to information related to services which were privately paid for by patients. Since most clinical information systems do not differentiate information based on who pays for the service, it will be very difficult to separate the information.

Typically, a patient's information within a clinical information system is associated with an encounter number. Charge information associated with services provided to a patient is passed along with the encounter number, from the clinical information system(s) to a separate billing system. The billing system then pairs the charge information with whoever is identified as being responsible for payment. Therefore, to restrict access to the information, the payer information must be passed to and retained within the clinical information system(s).

The other alternative would be for information associated with services that were privately paid for by patients to be separate from other information in the patient's record (such as establishing a separate medical record). In this case, unless there is a method to link the information together for treatment purposes, the clinician may not have access to all necessary information required for the effective and efficient delivery of health care.

Houston Question 3: *Mr. Houston, in your testimony you seemed to insinuate that de-identifying data would be too burdensome, time-intensive and costly.*

Are there no simple ways of removing the identifiable information? It would seem to me that because these are digital medical files the identifiable information could be easily removed using a computer.

What are your thoughts?

Response: While de-identification of data in structured data formats can be practically performed, studies have demonstrated that de-identification of unstructured data is not easily accomplished. “Unstructured data” is data that does not have a pre-defined format (i.e., such as name, address, date of birth, etc.), and is often found in “history and physicals”, progress notes, clinical messaging between staff, dictations, etc.

For example, it is not uncommon for diseases or medical devices to be named after individuals. To demonstrate this issue, an unstructured H&P might include the following: “Patient Hodgkin was diagnosed with Hodgkin’s lymphoma...” or “A Foley catheter was inserted in Patient Foley...” In each case, the software would need to select the appropriate name to remove. Removing the wrong information would result in medical information being removed from the de-identified record.

While these examples may appear straightforward, when removing all 18 identifiers as required by the HIPAA privacy rule, de-identification becomes much more difficult.

Houston Question 4: *The House bill directs the Secretary to promulgate regulations to eliminate activities from the definition of health care operations that could be conducted with deidentified information instead of individually identifiable protected health information.*

Could you talk about the types of activities, such as quality improvement, fraud and abuse detection, infection surveillance, disease management, etc. that fall under health care operations and indicate how the use of only de-identified or aggregate data could adversely impact these activities?

Response: I have a number of comments/concerns regarding the requirement to use de-identified data for health care operations.

- As indicated in my written testimony, there are far too many health care operations purposes to list. Attempting to identify all of these purposes and ascribing a de-identification standard to each will likely be incomplete, error-prone and impose a substantial burden on providers. This will create difficulty in terms of both de-identifying information, and determining which health care operations purpose requires de-identification.
- In your question you listed four health care operations purposes. Infection surveillance, for example, may involve performing trend analysis in some cases, but in others, it may involve a detailed review of patient records from multiple sources. In the former case, the use of de-identified or aggregate data may be perfectly acceptable. In the latter case, de-identified or aggregate data may prevent a complete investigation from being performed.

- In reading the definition of “health care operations” in the HIPAA privacy rule, there are many examples listed that make it clear that identifiable information is necessary. For example, in the HIPAA Privacy Rule, “conducting training programs” is listed in the definition of “health care operations”. There are many examples where the training requires that students come in direct contact with patients and the patient’s identifiable information.
- Health care operations activities often spontaneously occur during the delivery of health care services to our patients. As such, in many cases there is no opportunity to de-identify the information.

Houston Question 5: *I am concerned that the proposal in the House bill (stimulus package) that expands HIPAA's accounting for disclosures requirement reflects an unrealistic sense of hospitals' ability to account for disclosures*

This proposal calls for a sweeping expansion of HIPAA's current accounting for disclosures requirement to include non-oral disclosures for treatment, payment and operations. Intermountain Healthcare, a very sophisticated health IT user, tells me that it would cost approximately \$250 million over three years to develop the capacity to move toward compliance with the new requirements. (Programming and other set-up cost approach \$68 million; storage costs for maintaining a rolling period of three years of audit data would be approximately \$78 million; Infrastructure development and maintenance costs, including personnel for managing the audit data, would cost approximately \$106 million.) The current HIPAA rule rejected this approach because these disclosures are so routine, so fundamental to the delivery of health care, and so voluminous.

Can you tell me how the proposal to expand the accounting for disclosures requirement to include all non-oral disclosures of protected health information for treatment, payment and health care operations would impact UPMC?

Do you have a sense of how much it would cost to implement this provision?

Response: Based on the few cases where an accounting of disclosures has been requested, I do not believe that the cost to support this requirement is justified.

UPMC has yet to complete an analysis on the cost to address this requirement. However, the effort to consolidate and manage the information associated with providing such accounting of disclosures will be substantial, especially for large and technologically advanced health systems like UPMC. UPMC, like most large and technologically advanced health systems, does not employ a single large clinical information system. Rather, UPMC has upwards of 100 clinical information systems that are used to deliver care.

As required by HIPAA, UPMC currently tracks user access to patient information through its clinical information systems. For UPMC’s enterprise clinical information systems, UPMC has implemented a computer system that collects and consolidates user access logs, which are then provided to management staff so that user access can be review. This system cost UPMC \$500,000 to implement. Maintaining logs for extended periods of time will result in substantial additional storage cost.

Houston Question 6: *In the five years since the HIPAA Privacy Rule took effect, how many requests has UPMC had for an accounting for disclosures?*

How does that number compare to the number of patients for whom UPMC has provided care?

Response: While I cannot provide an exact number of requests, through a poll of our facilities' privacy staff, there was only one request for an accounting of disclosures in the last twelve months. As a health system with 20 hospitals and 400 outpatient sites and doctors' offices, during the same 12-month period, UPMC had over 3,000,000 outpatient, inpatient and physician office visits.

Houston Question 7: *Should breach notification requirements incorporate a risk-based standard (such that affected individuals are notified only when there is a reasonable likelihood of harm that could occur as a result of a breach of personal health information)?*

Response: A risk-based approach would be more appropriate. Properly implemented, such an approach would balance the need to inform patients of potential harm, without subjecting entities to seemingly punitive and unconstructive reporting. It is important to note that UPMC has historically notified its patients in the event that there has been a breach. Even before the enactment of state laws concerning this subject, UPMC's process was to communicate directly with affected patients and to underwrite the cost of credit monitoring services for one year and that remains our policy.



1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
<http://www.cdt.org>

Health IT: Protecting Americans' Privacy in the Digital Age Witness Questions from The Honorable Arlen Specter

Questions for Ms. McGraw, Dr. Hester and Ms. Hahn

1. Do you believe the privacy provisions that are part of the Health IT legislation that has been inserted into an appropriations bill through a closed-door process would benefit from going through regular order as is required of most Senate legislation?

Congress is proposing to spend \$20-23 billion to promote health information technology (Health IT) adoption and implementation as part of the economic recovery legislation. Health IT holds enormous potential to improve patient care and the efficiency of our health care system. Survey data shows that the American public supports health IT. At the same time, the public is very concerned about the risks that health IT poses to privacy. Building public trust in health IT systems is critical to reaping the technology's benefits.

We need a comprehensive framework of privacy and security protections to build public trust in health IT. A commitment to spending significant federal dollars to advance health IT must be coupled with a strong commitment to privacy and security. As a result, it is critical that privacy provisions be part of any legislation that promotes the adoption of health IT.

The urgent need to ensure that the public's health information remains private and secure in e-health systems justifies the inclusion of privacy provisions in the economic recovery legislation.

2. What steps can be taken to improve patients' knowledge of their rights under existing federal legislation?

Under the current Privacy Rule, each covered entity, with certain exceptions, must provide a notice of its privacy practices, including patients' rights under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. However, more often than not, privacy notices are written in language that the average person cannot understand. Further, rarely do patients focus on the details of such notices, and many wrongly assume that the existence of a "privacy policy" means that their health information will not be shared, even when the policy and the accompanying consent form say just the opposite.

Thus, while the privacy notice required under HIPAA is an important tool for informing patients of their rights, there is more that can be done to improve patients' knowledge of their rights. The economic recovery bill takes a step forward by authorizing funds for the Department of Health and Human Services to educate both patients and their health care providers on their rights and responsibilities under HIPAA. The Obama Administration could go further and disseminate a model privacy notice to be used by entities covered by HIPAA. The Administration could also impose (or encourage) a "layered" notice approach, where patients are provided with a one-page, easy-to-read summary of the most critical of the Privacy Rule's provisions; entities must then make a longer, more detailed notice available for patients who have further questions or who need more information.

3. Do you believe that consumers are or will be properly aware of the steps taken to secure their electronic health records? In your view, would consumers be more comfortable with the adoption of health IT if their providers were required to describe the steps taken to secure electronic medical data, including, for example, the encryption of records and maintenance of access logs?

No, I do not believe that many consumers are aware of the steps that entities take to secure their electronic health records. All entities covered by HIPAA are required to adopt security protections, but the law does not require that consumers be provided with detailed information on an entity's security practices. (We assume that some entities do voluntarily provide information on security practices to consumers to demonstrate their strong commitment to security – but to the best of my knowledge, there has been no systematic study of this or the impact that it has on building consumer trust and adoption.)

We believe it would increase consumer trust if security requirements were strengthened and if consumers knew more about the security practices of entities that maintain or have access to their health data (as long as any information revealed about security practices did not inadvertently compromise an institution's ability to secure the information). But good security practices are not sufficient on their own to build public trust. We also need a comprehensive framework of privacy policies that clearly set forth who can access health information and for what limited

purposes, and that are more aggressively enforced. Robust security practices will do little to build public trust if our privacy policies and practices permit overly broad access to the data.

The Honorable Orrin G. Hatch
U.S. Senate Judiciary Committee
Health IT: Protecting Americans' Privacy in the
Digital Age
January 27, 2009

Question for all panel members

I strongly support health IT, but believe this must be done very carefully so that we give health care providers the proper incentives to adopt technology without increasing regulatory burdens and costs.

Many health care groups have expressed concerns that requiring new and untested privacy mandates could damage the ability of providers to communicate with patients about treatment options and alternatives.

They are also concerned that additional privacy requirements would add costs to the health care system, and actually discourage providers from adopting the very health IT we want them to use.

Do you share these concerns and how would you recommend Congress and the Administration prevent these problems from occurring?

Ensuring appropriate privacy and security protections for electronic health information may require covered entities to adopt stronger policies and practices. Such entities will also need to update their care delivery and business models in order to ensure we reap the full benefits of transitioning health care to the digital age. These changes will not occur without some effort by industry, and we applaud providing federal financial support to the health care sector (particularly for primary care practices and safety net hospitals and delivery systems) to help us achieve a better, more interconnected health care system.

CDT believes the privacy provisions in the economic recovery package take workable, concrete steps toward the realization of a comprehensive framework of privacy protections that builds trust in health IT. These provisions build on the HIPAA Privacy and Security rules, a regulatory environment that is familiar to the health care industry, and do not impose a new and unfamiliar privacy infrastructure. The provisions in the bill also were carefully crafted to avoid imposing burdens on the health care industry that outweigh their benefits. Further, in circumstances where new functionalities are required to be adopted, the Secretary is tasked with developing regulations that further detail the requirements on industry, and he or

she must take into account the administrative and cost burdens on industry, as well as the potential impact on health care, in the development of these regulations.

As health IT is more widely disseminated, it will be critical for Congress and the Administration to continue to monitor developments to ensure that health IT is being effectively deployed to improve health care, and that adequate and workable privacy and security protections remain in place.

The Honorable Orrin G. Hatch
U.S. Senate Judiciary Committee
Health IT: Protecting Americans' Privacy in the
Digital Age
January 27, 2009

Question for all panel members

While I support a strong commitment to patient privacy, I am worried that some of the proposals under consideration would have unintended consequences for patients, physicians, and hospitals.

Specifically, I am particularly concerned about a proposal that would *prohibit* the use or disclosure of protected health information for routine health care activities without individual consent.

What are your thoughts on this type of proposal?

Any thoughts on how a prior consent requirement would affect patient care, quality improvement and research?

Requiring patient consent for every routine use of health care information provides very weak protection for privacy, unnecessarily burdens patients, and creates obstacles to the sharing of information within the health care system for important health care purposes. CDT does not support an approach to privacy that relies too much on patient consent, and there is no such provision in the economic recovery legislation.

Although patient consent is not a panacea, it is one component of a comprehensive framework of privacy and security provisions that should govern the sharing of health information. We believe health information should be allowed to flow without requiring patient consent for core health purposes, including treatment, payment, and those limited administrative functions that are critical to care delivery and payment. At the same time, health IT enables us to provide consumers with opportunities to make more meaningful choices about the use of their health data.

As a result, we need a strong role for patient consent with respect to access and disclosure of information in personal health records. Patients should also have choices with respect to whether or not their health records are part of a state, regional or national health information exchange. We also need to ensure that where patient consent is required, our health IT systems have the capacity to honor that consent.

With respect to the use of patient information for health care quality activities, we share your concerns about requiring consent or authorization for the use of this information, particularly when the quality assessment and improvement activities take place within an institution or an organized and integrated delivery system. However, we also believe that it is not necessary to use fully identifiable patient data for quality assessment and improvement functions, and that entities conducting such activities should be able to accomplish their purposes using data that has been anonymized or masked, which provides greater protection for privacy.

With respect to research, the HIPAA Privacy Rule permits a covered entity to use and disclose protected health information for research purposes in certain circumstances without a patient's consent, where the risks to privacy are minimal. The economic recovery legislation does nothing to alter these research rules (although early drafts do limit the remuneration received for such research to the costs associated with gathering and transmitting the data). A covered entity may disclose health information without patient consent to researchers if the researcher: (1) has obtained authorization from an Institutional Review Board or Privacy Board to proceed without consent; or (2) represents to the covered entity that he or she is seeking health information solely to prepare a research protocol or to conduct an activity preparatory to the main research (and he/she does not remove the health information from the premises); or (3) represents that he or she is seeking only the health information of someone who is deceased and the information is necessary for the research. Covered entities may also use or disclose, without an individuals' authorization, a limited data set of information for research purposes. Limited data sets are data that has been stripped of common patient identifiers, which greatly reduces the risks to privacy.

The Honorable Orrin G. Hatch
U.S. Senate Judiciary Committee
Health IT: Protecting Americans' Privacy in the
Digital Age
January 27, 2009

Question for all panel members

Throughout all of your testimonies you all agreed that it is essential that there be privacy protections in place as we move nationally toward health IT. But, it seems that most of the

ideas discussed were rather broad.

Do you have any specific suggestions as to what privacy protections should be considered?

Privacy Solutions That Enable Health IT

- **Ensure that all entities that collect, store or manage personal health information are required to comply with baseline health information privacy and security protections:**
 - **Adopt a broad policy framework based on fair information practices that governs all federal efforts to advance health IT.**
 - **Ensure that traditional health system entities who are covered by HIPAA and entities that handle personal health information on their behalf (“business associates”) are at least held accountable to the minimum privacy and security standards in the HIPAA rules.**
 - **Ensure that health information exchanges (commonly known as HIEs or Regional Health Information Organizations (RHIOs)), which today are not covered under HIPAA, are required to comply with HIPAA requirements, either as covered entities or business associates depending on their structure and functions.**
 - **Establish privacy and security protections for personal health information stored with or managed by non-health care entities (such as employers and Internet companies). It is neither sufficient nor effective to extend the HIPAA Rule to these entities. Instead, Congress will probably have to pass a statute with some parameters and authorize the FTC, in consultation with HHS, to develop and enforce appropriate protections.**
- **Establish a federal, individual right to be notified in the event of a breach of identifiable health information; such a requirement should probably include an exemption for information that is encrypted.**
- **Ensure appropriate standards are in place for the use of data that has been stripped of identifiers so that it is anonymous to the data holder. Includes revisiting the current standards in the Privacy Rule for de-identification and use of what are called “limited data sets” to ensure they continue to minimize the risk of re-identification while serving the needs of researches and others, and establishing penalties for re-identification that apply to all data recipients.**
- **Establish clear rules regarding the use of personal health information for marketing and commercial purposes that are not solely reliant on patient authorization. Includes tightening the definition of marketing in the Privacy Rule**

for HIPAA covered entities, as well as setting clear standards for the use of data for marketing and other commercial purposes by non-health care entities.

- **Ensure strong oversight and accountability for all entities handling health information. Will require strengthening HIPAA enforcement by: (1) clarifying the HIPAA statute so that criminal penalties can be imposed against individuals, and to ensure civil monetary penalties are imposed in cases of willful neglect of the rules; and (2) providing additional enforcement resources, such as through an increase in appropriations to HHS and/or by expressly authorizing states to enforce. Will also require FTC to take a more active role to ensure enforcement of consumer protections against non-health care entities.**
- **Revisit the scope of the concept of "health care operations," a category of uses under the current Rule that does not require patient authorization. Reconsideration of the scope of the exception is particularly appropriate for situations where data is shared outside of a HIPAA-covered health care entity for such purposes. Require the use of anonymized data for health care operations that do not need identifiable data. Consider whether some purposes under "operations" should require patient authorization.**
- **Strengthen the role of patient consent by requiring opt-in before patient health information is stored in or shared through an electronic health information exchange, particularly where the exchanges are used for purposes beyond treatment, and by ensuring that health information stored in personal health records and other consumer-facing tools is accessible only with patient authorization. Consider also strengthening the HIPAA "right to restrict" the access and disclosure of health information, particularly for more sensitive health data.**
- **Ensure individuals can promptly obtain electronic copies of their health information from health care providers and plans and require entities with electronic health record systems to provide audit trails of uses and disclosures to individuals upon request.**
- **Devote more resources to education about health privacy and the protections under current law, for both patients and for those required to comply with the laws, and develop and disseminate model privacy notices (a one-page summary notice and a longer, more detailed notice) that more clearly explain how information can be used and disclosed and patient's rights under current law.**

The Honorable Orrin G. Hatch
U.S. Senate Judiciary Committee

Health IT: Protecting Americans' Privacy in the
Digital Age
January 27, 2009

Question for all panel members

Greater adoption of health IT has been recognized as enabling improved chronic disease management through better coordination of care. In order to coordinate care, providers need to be able to have access to patient data collected via health IT.

For example, a provider could generate a list of all diabetic patients in a practice to ensure screening tests are up-to-date, prescriptions are filled, or to determine if any patients are overdue for a visit.

What impact could privacy restrictions have on this and other care coordination functions?

Currently, there is nothing in the bill's provisions that would hamper a provider's access to health information for these purposes. Many of these, when done by a provider, would be considered part of treatment – and the bill does not change the ability to use information for treatment purposes.

To the extent that these activities are considered health care operations under HIPAA, the bill tasks the Secretary with reviewing the scope of the category of health care operations, and CDT supports a thorough review. Currently, the category is too broad, particularly with respect to the sharing of identifiable data for operations purposes outside of a HIPAA-covered health care entity (see footnote below for a complete list of the activities within health care operations).¹ Under HIPAA regulations today, fully identifiable data can be used for any health care operation, and many of the activities in operations could be done with anonymized data (allowing the entity to get what it needs from the data but also providing greater protections for patient privacy). There may also be some components of operations that should require patient authorization. Giving the Secretary the full discretion to

¹ Health care operations include: (1) Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination; (2) Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities; (3) Underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims; (4) Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs; (5) Business Planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and (6) Business management and general administrative activities, including those related implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity. 45 C.F.R. §164.501.

review this category as part of a regulatory process, which allows all stakeholders to weigh in with any concerns, is the appropriate way to address this issue.

The Honorable Orrin G. Hatch
U.S. Senate Judiciary Committee
Health IT: Protecting Americans' Privacy in the
Digital Age
January 27, 2009

Question for all panel members

I have heard concerns expressed that by putting very narrow privacy constraints on the use of health information – like allowing specific information to be hidden and permitting medical treatment paid out-of-pocket to be kept secret – you encourage greater fraud and abuse, increase the incident of improper payments, and double-billing, among other things.

What is your take or reaction to those concerns and what solutions, if any, would you propose?

Under the current Privacy Rule, patients have the right to request a restriction on uses and disclosures of their personal health information for treatment, payment, and health care operations. However, a covered entity is under no obligation to grant the request. Therefore, though patients have a right to restrict, this right is not very meaningful.

In cases where a patient wants to pay for health care out-of-pocket, CDT believes a covered entity should honor a request not to disclose information related to that care to an insurer specifically for payment purposes. By failing to honor a patient's request to restrict, a covered entity sending a claim for a service that had been paid in full would not only be committing fraud; it would also be violating the HIPAA Privacy Rule.

Electronic systems, which have greater tracking and segmentation abilities, can help entities better comply with these restrictions in the limited instances when they are requested and can help auditors detect fraud and double billing. Most people with insurance want their care to be paid for by the insurer; only those with heightened privacy concerns, or who are seeking particularly sensitive care (such as mental health or substance abuse) will seek to take advantage of this.

As a final note, strengthening protections against insurance and employment discrimination based on actual health condition, or health information, would also help address people's concerns about access to their sensitive health information.

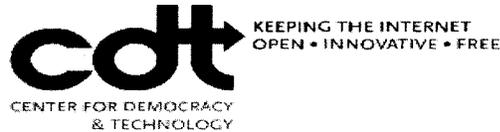
Question for Deven McGraw - Director, Health Privacy Project, Center for Democracy and Technology:

When a patient requests a copy of an electronic health record from a medical care provider, some have discussed allowing a copy of that record to be sent directly to a personal health record, as opposed to just the patient, if the patient chooses that route. Those advocating this view believe that sending information directly to the PHR will result in better management of health care, cost-saving opportunities, and a lesser chance that the data would be lost in transmission. What is your opinion?

We agree with giving patients the right to have a copy of their information sent directly to the personal health record (PHR) of their choice, and we have supported that language be added to the legislation to expressly provide for this. If such language is not added in the legislation, we will urge the Administration to make this clear in HIPAA regulations or in guidance.

With respect to PHRs, we believe that more work will also need to be done to ensure that the health information in these records is adequately protected. PHRs provide patients with unique opportunities to get engaged in, and manage, their own health care. PHRs and other consumer access services and tools are now being created by both covered entities, and by non-covered entities, including Internet companies like Google and Microsoft. Since the latter are not covered by HIPAA, patient privacy in this arena is only protected by the PHR provider's privacy and security policies (and potentially under certain state laws that apply to uses and disclosures of certain types of health information), and if these policies are violated, the FTC may bring an action against a company for failure to abide by its privacy policies.

CDT recognizes the benefits of PHRs, but also sees a need for greater privacy protections within this arena. To achieve this, CDT does not support the idea of expanding the HIPAA Privacy Rule to cover these non-covered PHRs because it would not provide adequate protection for PHRs, and may do more harm than good in its current scope. Instead, CDT supports the HHS and FTC agencies jointly creating recommendations for privacy and security requirements for this arena, which is already in the legislation.



December 18, 2009

Responses of Deven McGraw, Director, Health Privacy Project
 Questions posed by Senator Patrick Leahy, Chairman, Senate Judiciary Committee
 Hearing: "Health IT: Protecting Americans' Privacy in the Digital Age"

1. **Enforcement of the privacy and security rules under the Health Information Portability and Accountability Act ("HIPAA") was lax under the Bush Administration. According to statistics from the American Psychoanalytic Association, the Bush Administration failed to impose a single civil monetary penalty for violations of the HIPAA privacy rule despite receiving close to 40,000 privacy complaints since 2003. How can Congress and the Obama Administration ensure enforcement, accountability, and transparency of the Nation's health privacy laws?**

In the American Recovery and Re-investment Act of 2009 (ARRA), Congress took a number of steps to strengthen HIPAA enforcement, such as by expressly authorizing state attorneys general to enforce HIPAA through civil enforcement actions, increasing civil penalties for HIPAA violations, putting business associates in direct responsibility for complying with key HIPAA privacy and security provisions, and requiring HHS to impose civil monetary penalties in circumstances where it finds that a HIPAA violation was willful (Sections 13409-13411). Unfortunately, HIPAA still does not include a private right of action, leaving individuals dependent on government authorities to vindicate their rights under HIPAA.

Moving forward to ensure comprehensive protection of health privacy will require strong commitment to enforcement from both the government and the private sector. Several of ARRA's key provisions require rulemaking by the Secretary of HHS to specify details, and carefully crafted regulations and other guidance to flesh out statutory requirements can make a significant impact on accountability and transparency of health information management. HHS should work closely with the FTC to ensure enforcement of health privacy laws for entities not covered under HIPAA.

Successful implementation of the new federal rules will also require industry initiative, standards activity, and legislative oversight. The Act creates two advisory committees, one on policy and one on standards, to advise the Secretary on implementation issues, which should include effective enforcement for

1

violations. Finally, allocating the \$19 billion in HIT funding will require careful attention to ensure that funding recipients have the technical capability and commitment to safeguard patient privacy and make the most of HIT's benefits.

2. **Data security should be a high priority when American' sensitive health information is sold or shared to third parties. Yet, currently consumer health information stored on web-based personal health records is not subject to HIPAA, the nation's main federal health privacy law. As a result, the health privacy and security protections offered in HIPAA do not apply to data brokers who access personal health information through this new technology. What can Congress do to protect a patient's sensitive health information if, and when, it is shared with unregulated commercial data brokers?**

ARRA does not establish privacy rules for personal health records (PHRs) and other Internet-based services that operate outside the traditional healthcare structure. For PHRs to flourish, CDT believes clear rules are needed for marketing and commercial uses of information that will better protect consumers by restricting PHR vendors from engaging in certain practices, or by providing individuals with certain rights – essentially a stronger and more comprehensive package of privacy and security safeguards than mere consent. This may mean the application of certain provisions in HIPAA, but it is CDT's view that merely extending HIPAA to PHRs is insufficient.

Instead, rules need to be crafted that are tailored to the unique issues posed by patient-controlled records. ARRA requires HHS to work with the Federal Trade Commission (FTC) and report to Congress on privacy and security protections that should apply to PHRs. This report, which must be submitted no later than February 17, 2010, must also consider which agency is best equipped to enforce the recommended protections and a timetable for further regulation. CDT believes the FTC's experience and track record with commercial data brokers make it the most appropriate entity to enforce health privacy regulations for entities not covered under HIPAA.

Possibly the best thing Congress can do to protect the privacy of health information in the commercial context is to pass general consumer privacy legislation that is based on a full set of Fair Information Practices (FIPs). Industry self-regulation does not adequately protect privacy without stronger legal standards and more direct oversight from the FTC, state attorneys general and other enforcement bodies. Congress should consider granting the FTC standard rulemaking authority, as many other agencies have under the Administrative Procedure Act. The collection, use and distribution of personal data is widespread and growing rapidly; now is the time for Congress to take an active role in developing a comprehensive privacy framework for the next decade.

3. **The HIPAA privacy rules were a landmark in privacy protection – they were the first federal health privacy protections ever enacted and implemented.**

Yet, today we have technology and Internet-based companies developing tools and websites that collect, store and/or manage personal health information, and they are not covered by any federal health privacy law. What changes to HIPAA would better safeguard Americans' sensitive and valuable health records in the Digital Age?

In the PHR arena, consumer privacy is only protected by the PHR offeror's privacy and security policies (and potentially under applicable state health information laws), and the company may be subject to FTC action and if those policies are violated. The policies of PHR vendors range from very good to seriously deficient.

This dynamic is motivating some to suggest extending HIPAA to cover all PHRs. However, CDT believes the HIPAA Privacy Rule, which was designed to protect information exchanged among *traditional health care entities*, does not provide adequate protection for PHRs. Under the HIPAA Privacy Rule, personal health information is permitted to flow without patient authorization for a variety of purposes related to treatment and payment for care; other uses, some of which spark serious privacy concerns among patients (i.e., marketing, disclosure to employers), require express patient authorization.

Bringing the regulation of PHRs under the Privacy Rule would authorize the disclosure of sensitive data outside the healthcare system, subject only to patient authorization. Such broad reliance on consent unfairly shifts much of the burden of protecting privacy on the individual and puts the bargaining power on the side of the PHR offeror.

If, however, the joint HHS-FTC report required under ARRA concludes that the Privacy Rule is the best vehicle to strengthen protections for consumers who use PHRs, CDT believes the HHS Secretary should promulgate rules specific to PHRs that respond to the unique issues raised by these tools, rather than twist existing regulations for traditional healthcare entities to encompass PHRs also. For example, the rules permitting covered entities to use personal health information without express authorization for treatment, purposes and healthcare operations should not be applied to PHRs.

U.S. Senate Judiciary Committee*"Health IT: Protecting Americans' Privacy in the Digital Age"*January 27, 2009

Responses to Written Questions Requested by the Committee

Submitted by David Merritt

From Senator Hatch:

I strongly support health IT, but believe this must be done very carefully so that we give health care providers the proper incentives to adopt technology without increasing regulatory burdens and costs.

Many health care groups have expressed concerns that requiring new and untested privacy mandates could damage the ability of providers to communicate with patients about treatment options and alternatives. They are also concerned that additional privacy requirements would add costs to the health care system, and actually discourage providers from adopting the very health IT we want them to use.

Do you share these concerns and how would you recommend Congress and the Administration prevent these problems from occurring?

Yes, this is a real concern. A delicate balance needs to be struck between privacy on one hand and treating patients with the most modern tools on the other. In short, we need to find the right balance between privacy at all costs and progress at any cost.

Two issues exemplify the tension: patient consent and data breach notification. Patients should have a legal framework that includes the right of individual consent. Individuals should have the opportunity to opt-out of certain products, services, or notifications and specify how their specific identifiable information can or cannot be shared outside the course of treatment or payment. This consent can be balanced so that it does not impose new, undue burdens on providers, health plans, and other entities.

As I outlined in my written testimony, one way to accomplish this may be through a uniform patient consent form. Such a form could specify standards and instructions that "clearly reflect patients' rights to information in their

medical records and provider confidentiality principles.”¹ Such a form could be collected at the time of enrollment in a public or private health plan or before services are delivered.

Patients should also be notified of egregious breaches of privacy and security. And to achieve a balance between informing patients and not complicating the treatment process, the standard for what defines a breach must be set very high. Protections should incorporate a risk-based notification, so that physicians, health plans, and health systems do not notify patients for harmless or inadvertent data sharing. If, for instance, a physician mistakenly sees the record of a patient he or she is not treating, should that qualify as a data breach? Should the patient whose record was seen be notified? The bar should be set very high so that these types of cases do not generate unnecessarily notifications.

The two important issues, as well as many others, should be carefully considered through the rule-making process. There must be a balance between protecting patients and process requirements for health plans, physicians, and other providers.

Question from Senator Specter

You testified that enforcing privacy violations must strike the correct balance between patient privacy and creating a new legal market for frivolous lawsuits. Do you believe that this balance would be disrupted if Congress authorized state attorneys' generals to bring federal HIPAA privacy enforcement actions in federal court for statutory damages and attorneys' fees?

Yes. Under current law, HIPAA may only be enforced by the federal government. This means that HIPAA policy is uniform, that decisions to sue are uniform, and that there no extraneous financial reasons to sue doctors or hospitals. Delegating this responsibility to states and permitting them to re-delegate to private attorneys upsets this equation.

First, it will disrupt national uniformity because each state and each private attorney will be interpreting the law differently. Federal laws should be uniform; with these changes, HIPAA would not longer be. Second, the amendment would interject the private financial considerations of the private attorney into what ought to be a purely legal decision. This is especially so where the attorney is paid on a contingency fee. Third, it will drive up healthcare costs without providing any direct benefit. It may in fact create “defensive information sharing,” where doctors treating the same patient are reluctant to share information with each other about that patient. This would actually endanger patients.

¹ RTI International, *Privacy and Security Solutions for Interoperable Health Information Exchange: Assessment of Variation and Analysis of Solutions*, July 2007. http://www.rti.org/pubs/avas_execsummi.pdf (Accessed January 24, 2009.)

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
<http://www.microsoft.com/>



March 5, 2009

The Honorable Patrick Leahy, Chairman
Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Orrin G. Hatch
Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

Re: Written Questions Following Hearing on
"Health IT: Protecting Americans' Privacy in the Digital Age"

Dear Chairman Leahy and Senator Hatch:

Thank you for the opportunity to testify at the Senate Judiciary Committee's January 27, 2009, hearing on "Health IT: Protecting Americans' Privacy in the Digital Age." Privacy issues will continue to be important as organizations and agencies work to implement the health IT provisions in the American Recovery and Reinvestment Act ("ARRA") and to bring about real change in our healthcare system.

Microsoft believes that strong privacy protections are not only compatible with bringing the benefits of health IT to patients, providers, and healthcare organizations, but are essential to ensuring the future of the U.S. healthcare system. As my testimony emphasized, data liquidity can drive new therapies, new cures, and new lessons about disease, but patients will only be comfortable sharing health data if they feel confident that their health privacy is being protected.

This means that Microsoft, and all organizations that use or provide health IT, must adopt meaningful privacy practices that build trust with consumers. To do this, we must be transparent about what health data is collected from patients and how such data will be used; we must offer patients controls over the use and disclosure of their health data; and we must protect health data from unauthorized access.

Microsoft looks forward to cooperating with the public and private sectors to build the principles of transparency, control, and security into health IT systems, thereby establishing the trust that is critical to the success of health IT and healthcare in general.

Your follow-up questions raise interesting and important issues. Please find below our responses to the specific questions you have asked.

I. **Chairman Leahy's Written Questions for Michael Stokes**

1. Web-based personal health records were created to empower consumers to be more actively engaged in their own health care. This new technology enables ordinary persons to store and control their medical data on-line. Yet, serious concerns have been raised about the potential breach of privacy and security of on-line personal health records. A report issued last February by World Privacy Forum found that storing health records on-line can be counterproductive to safeguarding consumer privacy; it can open the door for sensitive health data to be easily accessible to hackers and shared by commercial data brokers outside the health care system. Your company recently launched a web-based personal health record database called HealthVault. How will Microsoft ensure that HealthVault will adequately protect individuals' sensitive health records from inappropriate access or use?

Microsoft recognizes that health data can be highly sensitive, and we are committed to protecting the privacy of that data. In HealthVault, we have implemented a series of safeguards based on the principles of transparency, control, and security.

- ***Transparency.*** HealthVault provides a clear, easy-to-read privacy notice. The notice tells users how, where, and why Microsoft uses personal data collected through HealthVault. It also explains when and why a third party might request access to personal data.
- ***Control.*** HealthVault gives individuals control over their own health records, enabling them to decide what goes into the record and who will be able to see, use, and share that data. HealthVault data is not shared with third parties unless the third party has disclosed what the data will be used for and the individual has affirmatively authorized the third party to access the data.
- ***Security.*** To protect against hacking and other illicit intrusions, Microsoft has implemented strong security measures. Our broad approach to protecting the security of personal information incorporates a wide array of technological and procedural protections, including independent security penetration testing, auditing and logging capabilities, controlled-access facilities, and encrypted Internet protocols when communicating personal health data. We have also partnered with industry, law enforcement, and consumer groups around the world to identify security threats and share best practices.

2. One of the areas of contention over health IT legislation is whether, and to what extent, patients should exercise control over the operation of their health care records. Consumer advocates tend to favor proposals that would allow consumers greater control over who accesses their information. Other stakeholders, however, contend that greater consumer control may jeopardize effective and high quality health care. What does Microsoft think about giving American consumers more control over their own health data?

For consumer services such as HealthVault, Microsoft believes in empowering consumers to be stewards of their own health data. HealthVault is based on the idea that consumers should be able to connect all their health and wellness data electronically, share it securely from provider to provider, and keep it in one place over time, no matter the doctor or the insurance company. Consumers using HealthVault already have the ability to access an audit trail that indicates who has accessed their records and what actions have been taken. When consumers understand who will be looking at their data, have control

over its dissemination, and feel confident that the data will be secure, they will be more comfortable entrusting their sensitive data to the healthcare system.

When it comes to clinical records, Microsoft provides technological tools that enable the custodian of the information to implement effective privacy controls. In enterprise solutions such as Amalga, Microsoft's software allows hospitals to comply with applicable laws and regulations and to customize their data policies as they see fit. The ARRA expands individuals' right to obtain an accounting of disclosures of their electronic health information, including disclosures for treatment, payment, or healthcare operations during the three prior years. Microsoft believes that the accounting requirement in the ARRA can be implemented in a way that provides consumers with meaningful information about disclosures of their health data without jeopardizing healthcare effectiveness, and we look forward to partnering with the public and private sectors in order to achieve this outcome.

II. Senator Hatch's Written Questions for All Panel Members

1. I strongly support health IT, but believe this must be done very carefully so that we give health care providers the proper incentives to adopt technology without increasing regulatory burdens and costs. Many health care groups have expressed concerns that requiring new and untested privacy mandates could damage the ability of providers to communicate with patients about treatment options and alternatives. They are also concerned that additional privacy requirements would add costs to the health care system, and actually discourage providers from adopting the very health IT we want them to use. Do you share these concerns and how would you recommend Congress and the Administration prevent these problems from occurring?

Microsoft agrees that privacy requirements need to be carefully designed so that they do not discourage providers from adopting health IT. Privacy protections based on the principles of transparency, control, and security can help ensure that both providers and patients trust, and are willing to participate in, the system.

In my role as Principal Program Manager for Microsoft's Health Solutions Group, I am responsible and accountable across the group for compliance with the Privacy and Security Rules promulgated under the Health Insurance Portability and Accountability Act ("HIPAA"). My understanding is that the HIPAA Privacy Rule and the new provisions under the ARRA still allow providers to discuss treatment options and alternatives with their patients without obtaining prior authorization to do so. Under HIPAA, communications that relate to the treatment of the individual, case management / care coordination, or recommendations for alternative treatments are not considered marketing and can be made without prior authorization. The ARRA appears to preserve these exceptions, so long as the provider is not being paid to make the communication. Moreover, even though the Act restricts payments for providing protected health information of an individual without consent, there are exceptions for treatment of the individual and for providing the individual with a copy of his or her medical record. In short, Microsoft believes that these new provisions will not damage patient-doctor communications. We will work with our business partners to analyze and comply with the new requirements.

Microsoft recognizes that there will be certain start-up costs associated with the new privacy requirements, as there are with most new regulations. In the long run, however, properly designed privacy protections can save money. Chief Information Officers at hospitals are already demanding technological tools that give them transparency into how health information is used and stored across their institutions, control over how that information is distributed, and secure methods of protecting

that information. These tools, which hospital CIOs need in order to improve quality and reduce costs, are the same technologies required to improve patient privacy. Effective privacy protections can foster the exchange and reuse of health data, which in turn can eliminate the need for unnecessary procedures, allow providers to make more accurate diagnoses, and contribute to important medical breakthroughs.

2. While I support a strong commitment to patient privacy, I am worried that some of the proposals under consideration would have unintended consequences for patients, physicians, and hospitals. Specifically, I am particularly concerned about a proposal that would prohibit the use or disclosure of protected health information for routine health care activities without individual consent. What are your thoughts on this type of proposal? Any thoughts on how a prior consent requirement would affect patient care, quality improvement and research?

Patients' health and well-being is the ultimate goal of the healthcare system, and Microsoft understands that privacy protections must be designed in a way that facilitates this outcome. The principles of transparency, control, and security can help create privacy safeguards that individuals both want and feel comfortable with. For example, two-thirds of Americans are willing to include their health data anonymously in a large database to help researchers.¹ When providers are transparent about the intended uses of the data—e.g., to help researchers—and when consumers can exercise control over how their data is shared—e.g., anonymously in a large database—better outcomes are achieved for everyone. Researchers have access to the data they need to make medical discoveries, and consumers benefit from research breakthroughs.

Under the ARRA, a covered entity cannot receive payment (either directly or indirectly) in exchange for providing protected health information without prior authorization. An exception is provided for, inter alia, the exchange of protected health information for public health activities, research, or treatment of the individual. Microsoft understands that the Department of Health and Human Services ("HHS") will be developing regulations to implement this provision, and we look forward to working with HHS and other healthcare participants to ensure that the new requirements do not hamper the delivery of effective patient care, quality assurance, and medical research.

3. Throughout all of your testimonies you all agreed that it is essential that there be privacy protections in place as we move nationally toward health IT. But, it seems that most of the ideas discussed were rather broad. Do you have any specific suggestions as to what privacy protections should be considered?

Microsoft appreciates the efforts made by Congress in examining and enacting the ARRA's privacy protections, and we are continuing to analyze the specific privacy provisions that were included in the legislation. Microsoft will work with HHS and others to ensure that regulations promulgated under the ARRA—including new regulations governing payment for the exchange of protected health information, breach notification, and the accounting requirement—bring the transparency, control, and security needed to drive changes in our healthcare system.

¹ Council for Excellence in Government et al., *The American Public on Healthcare: The Missing Perspective* (2008), <http://www.excelgov.org/Programs/ProgramDetail.cfm?ItemNumber=9404>.

4. Greater adoption of health IT has been recognized as enabling improved chronic disease management through better coordination of care. In order to coordinate care, providers need to be able to have access to patient data collected via health IT. For example, a provider could generate a list of all diabetic patients in a practice to ensure screening tests are up-to-date, prescriptions are filled, or to determine if any patients are overdue for a visit. What impact could privacy restrictions have on this and other care coordination functions?

Microsoft agrees that health IT can greatly benefit care coordination, and we are actively partnering with leading healthcare organizations to deliver novel improvements in chronic disease management. For example, our ongoing pilot project with the Cleveland Clinic is the first pilot in the country to follow multiple chronic diseases (specifically, diabetes, hypertension, and heart failure) in the clinical delivery setting using multiple at-home devices (e.g., glucometers, heart rate monitors, weight scales, and blood pressure monitors). Patients enrolled in the pilot upload device data to HealthVault using a home computer, and the Cleveland Clinic downloads the data into online charts accessible by treating physicians. Having data constantly monitored and shared in an efficient way can improve treatment decisions, quality of life, and management of acute care incidents.

Privacy protections can and should be designed to encourage these kinds of innovative uses of health IT. Appropriate privacy protections, based on the principles of transparency, control, and security, can actually improve care coordination functions. Once patients understand what their data will be used for, know who is looking at it and for what purpose, and are assured that their data is secure, they will be more inclined to share the health data that is needed for effective treatment and case management.

5. I have heard concerns expressed that by putting very narrow privacy constraints on the use of health information – like allowing specific information to be hidden and permitting medical treatment paid out-of-pocket to be kept secret – you encourage greater fraud and abuse, increase the incident of improper payments, and double-billing, among other things. What is your take or reaction to those concerns and what solutions, if any, would you propose?

As a general matter, Microsoft believes that effective privacy protections, including protections in the area of control, encourage patients to trust and participate in the healthcare system. However, Microsoft is concerned about a new provision in the ARRA under which individuals who pay out of pocket for a healthcare item or service can request that their data not be disclosed for payment purposes or not be used to conduct healthcare operations. A past study has shown that this kind of privacy-protective behavior can put individuals' health at risk.² Moreover, the restriction on the use of data in healthcare operations could negatively impact the availability of data for quality assurance and other vital healthcare functions. We believe that effective consumer education will be needed to help ensure that patients understand the consequences of hiding information and are willing to share health data with the providers who need that data in order to make sound medical decisions.

² California HealthCare Foundation, *National Consumer Health Privacy Survey 2005* (Nov. 2005), <http://www.chcf.org/topics/view.cfm?itemID=115694>.

III. **Senator Hatch's Written Questions for Michael Stokes**

1. Mr. Stokes, if I put my health data into HealthVault, what is Microsoft doing to protect the information it stores?

Microsoft recognizes that health data can be highly sensitive, and we have accordingly implemented strong measures to protect against the misuse of HealthVault data. One of our key principles is that individuals should control their own HealthVault data. Unless the individual gives explicit permission, data is not shared with third parties or others who seek to provide personalized ads or services.

In addition to the contractual protections we require from our business partners, Microsoft uses a wide array of technological and procedural protections to prevent hacking and other unauthorized intrusions. Our Security Development Lifecycle program calls for security evaluations and an appropriate combination of security measures, such as independent security penetration testing, independent certifications including ISO 27001, information segmentation, Lightweight Directory Access Protocol (LDAP) integration, auditing and logging capabilities, controlled-access facilities, and encrypted Internet protocols when communicating personal health data. We also work closely with industry, consumer advocacy, and law enforcement partners to improve our coordinated response to security issues.

2. Mr. Stokes, you talk a lot about the importance of sharing data in your testimony. Why is it important for patients to share data? Can I share some, but not all, of my health data?

As my testimony indicates, it is important for patients to share data because the future of connected, patient-centric healthcare depends upon the exchange and reuse of health data. Right now, patients' health data is locked in silos, forcing physicians to either make treatment decisions based on incomplete data or else waste time and resources aggregating information. A health IT system that allows patients to connect their health data and share it securely from provider to provider would allow physicians to see patients' complete health history. More reliable data in turn enables providers to make better medical decisions, decrease wasteful spending, and increase the quality of care.

In consumer services such as HealthVault, individuals can choose to share some, none, or all of their health data. In fact, Microsoft provides many different tools to help individuals control the sharing of their data. In addition to controlling what data is shared, HealthVault users can control the who, the how, and the when: They can decide who else should have access to that data, whether others are allowed to modify or only to view the data, and how long others can access the data. These tools give consumers the flexibility to adjust their access decisions as their health needs change.

3. Mr. Houston, in your testimony you seemed to insinuate that de-identifying data would be too burdensome, time-intensive and costly. Are there no simple ways of removing the identifiable information? It would seem to me that because these are digital medical files the identifiable information could be easily removed using a computer. What are your thoughts? Mr. Stokes, do you have an opinion on this matter?

Microsoft understands that de-identifying data in a way that robustly prevents re-identification is a difficult technical challenge. However, we believe that de-identified data can be used in transparent, controlled, and secure ways that protect individuals' privacy, and we are investing in active research to develop new innovations in this area.

* * *

Microsoft recognizes that the protection of consumer privacy is a continuous journey, not a single destination. We can and will continue to develop and implement new privacy practices and protections for consumers as health IT becomes more widely used. At the same time, Microsoft acknowledges that technology is only a part of a comprehensive approach needed to drive real change in our healthcare system. Other critical components include education, leadership in healthcare organizations, and meaningful public policy. We look forward to partnering with all participants in the healthcare ecosystem to move toward dynamic, trusted, and consumer-driven healthcare.

Sincerely,

Michael Stokes
Principal Program Manager
Health Solutions Group
Microsoft Corporation

AARP SUBMISSIONS FOR THE RECORD

**STATEMENT FOR THE RECORD
SUBMITTED TO THE
SENATE JUDICIARY COMMITTEE
ON
HEALTH PRIVACY**

January 27, 2009

**AARP
601 E Street, NW
WASHINGTON, DC 20049**

For further information, contact:
Paul Cotton/Jenny Gladieux
Government Relations & Advocacy
(202) 434-3770

On behalf of AARP's nearly 40 million members, thank you for holding this timely hearing on health information technology (health IT) and the privacy of health information. Health IT is an essential building block for health care reform. A properly-designed national system for health IT will advance quality improvement goals by enabling exchange of data on prescriptions, laboratory tests, and imaging procedures; developing evidence on the safety and effectiveness of treatments; and improving quality and safety reporting. To ensure success, we must harness health IT's enormous potential to improve the safety, effectiveness, and efficiency of care without compromising the confidentiality of personal health information and data security.

Health IT is a critical enabling tool to improve the quality and safety of health care.

Among its many advantages, health IT can help:

- Reduce medical errors by, for example, eliminating mistakes that arise from poor handwriting or lack of complete medical records;
- Provide access to a patient's essential health information at critical times, such as in emergencies when people cannot speak for themselves or gain access to their health information;
- Reduce the need for duplicate tests and procedures by helping to make necessary information available in "real time";
- Eliminate redundant paperwork and the need for patients to repeat medical history and demographic data at every medical encounter;

- Reduce health disparities through more uniform and standardized data collection across the variables – such as race and ethnicity, gender, geography, language preference and history of patterns of un-insurance, as well as education level and socioeconomic status – that are used to not only measure the existence of health inequities, but to develop solutions to address these health inequities;
- Enhance access to care for individuals who live in remote areas or those who require ongoing monitoring through non-face-to-face encounters via telemedicine technologies;
- Facilitate use of a wide array of technologies that help people stay in their own homes and out of institutions;
- Support patients in managing their own care by offering them ready access to their personal health information;
- Allow caregivers and providers to better coordinate care;
- Let people who live far from aging parents take better care of them through real-time communication with providers and family members; and
- Facilitate analysis of aggregated, de-identified data, to more quickly reveal the most effective treatment options as well as public health threats.

In addition to these quality improvements, health IT has the potential to help save billions of dollars. The Congressional Budget Office has estimated that if use of health IT were a Medicare condition of participation for both physicians and hospitals, the federal government could save almost \$34 billion over 10 years.

Privacy

Americans want the benefits health IT can provide and support its use. A November 2007 *Wall Street Journal* poll found that three in four adults agreed that patients could receive better care if doctors and researchers were able to share information electronically. Two in three say sharing records could decrease medical errors, and nine in ten say patients should have access to their own electronic records maintained by their physician.¹

Notwithstanding recognition of its value, the American public is also wary of health IT because they are concerned about protecting the confidentiality of their personal health information. While many agree that information stored in electronic records is safer than in paper records, the public's concern about health IT is heightened with every breach of personal information they hear about in the media. Therefore, unless we can instill consumer confidence in health IT through strong privacy and security safeguards, the public will be reluctant to support wider adoption of health IT.

Fortunately, effective protections that have widespread support among a broad range of stakeholders can be implemented. For example, diverse groups who participate in the Markle Foundation's Connecting For Health initiative have

¹ Benefits of Electronic Health Records Seen as Outweighing Privacy Risks, *Wall Street Journal*, Nov. 29, 2007, <http://online.wsj.com/public/article/SB119565244262500549.html>

agreed on core privacy principles that can incorporate policy and technology tools to achieve meaningful safeguards for consumer privacy and data security.

Implementing a comprehensive framework of privacy and security protections for electronic personal health information is critical to building public trust in health IT. We need not choose between health IT and implementing effective protections for personal health information and ensuring data security. However, we do need to avoid simplistic, but ineffective, approaches. For example, requiring patient consent any time personal records are shared may appear reasonable and effective, but in fact may be unworkable in practice, have unintended consequences such as promoting blanket consents that weaken protections, be considered a "nuisance" by some, and create a false sense of security. We need a package of privacy policies and technology tools designed to address consumer privacy and data security, including measures that limit data collection and use, ensure patient access to their personal health information, and provide rigorous user authentication and other appropriate mechanisms to address data security, including effective remedies in the event of breach.

Because of the complexity of establishing workable privacy protections, AARP believes the best approach is to have Congress -- after establishing a broad set of parameters that establish policy direction -- charge an advisory board, established under Federal Advisory Committee Act rules, with developing the bulk of needed privacy policies. This structure would ensure openness and accountability in the

development of recommendations for privacy protections and data security. Given the difficulty Congress has faced in the past in achieving consensus on these issues, we believe that authorizing an advisory board whose mandate requires full transparency in its operations would advance the development of the privacy infrastructure we envision, which, in turn, will accelerate adoption of health IT.

Conclusion

We must harness health IT's enormous potential to improve the safety, effectiveness, and efficiency of care without compromising the confidentiality of personal health information and data security. We need Congress to act to establish broad policy parameters for privacy and security, and an advisory committee to fill in the details. We commend this Committee for working to strengthen incentives for widespread adoption of HIT, and we look forward to working with you and all of Congress to ensure passage of strong HIT legislation this year.



January 27, 2009

Chairman Daniel K. Inouye
Committee on Appropriations
U.S Senate
The Capitol S-131
Washington, DC 20510

Ranking Member Thad Cochran
Committee on Appropriations
U.S. Senate
The Capitol S-131
Washington, DC 20510

Dear Chairman Inouye and Ranking Member Cochran,

I am writing on behalf of the American Council of Life Insurers (ACLI) to express our grave concern with a number of the privacy and security provisions in Title XIII of the proposed Senate Appropriations stimulus bill. ACLI's 353 member life insurance companies account for approximately 93% of the industry's assets and 93% of life insurance premiums. ACLI member companies are also major participants in the nation's long term care and disability income insurance markets.

ACLI and its member companies recognize consumers' heightened concerns with the privacy of health information and have implemented robust procedures for protecting the privacy of such information. ACLI believes that certain privacy provisions in the stimulus legislation could jeopardize life insurers' ability to perform fundamental insurance business functions, ultimately to the detriment of policyholders. Therefore, ACLI urges that the proposed privacy provisions not apply to life insurers.

In view of the multitude of existing state and federal laws relating to privacy that already require life insurers to protect consumer health information, the proposed legislation would be duplicative of existing protections. In fact, unless the provisions of the draft legislation provide uniform preemptive national standards, life insurers could be left with requirements that are at odds with the requirements of many states and inconsistent with existing federal privacy standards adopted by agencies under the Gramm-Leach-Bliley Act.

ACLI and its member companies are deeply committed to the principle that individuals have a legitimate interest in the proper collection and handling of their personal medical information and that life insurers have an obligation to assure individuals of the confidentiality and security of that information. However, in light of the significant concerns described above, ACLI respectfully opposes Title XIII as currently written. We look forward to working with you and your staff as this legislation moves forward.

Sincerely,

Frank Keating
President & CEO

Cc: Chairman Ted Kennedy, Senate HELP Committee
Chairman Patrick Leahy, Senate Judiciary Committee
Ranking Member Michael Enzi, Senate HELP Committee

January 27, 2009

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20505

The Honorable Arlen Specter
Ranking Member
Committee on the Judiciary
United States Senate
Washington, D.C. 20505

Re: Hearing on "Health IT: Protecting Americans' Privacy in the Digital Age"

Chairman Leahy and Ranking Member Specter:

The American Psychoanalytic Association respectfully requests that the its paper, "Myths, Facts and Law About Health IT And The Right To Health Information Privacy" be included in the record and considered in the hearing today before the Judiciary Committee on Health IT: Protecting Americans' Privacy in the Digital Age". Since this is a hearing before the Judiciary Committee, we thought it might be appropriate for the Committee to have some information on the law of health information privacy at the state and federal levels and as reflected in federal case law.

We note that a recent "report" by one of the witnesses on the role of consent in protecting health information privacy does not discuss or even mention (a) the extensive Constitutional case law on the right to information privacy at the federal and state levels, (b) the fact that consent is a core concept of the ethical standards for nearly every segment of the medical profession, (c) that most states recognize a physician-patient privilege and that all 50 states and the District of Columbia and the U.S. Supreme Court have recognized a psychotherapist-patient privilege that can only be waived with patient consent, or (d) that all 50 states and the District of Columbia recognize a right to information privacy under tort law. Further, as the courts have noted, most Americans want and expect to have the

right to not have their personal health information disclosed without consent or over their objection.

As the case law listed in the Myths, Facts, and Law paper shows, the right to privacy of personal information is a fundamental constitutional right the essence of which is the right to control who sees one's personal information. Consent is the means by which this right of control is exercised. If there is no right of consent for routine uses and disclosures of health information, there can be no right to privacy with respect to those uses and disclosures. At a time when there are weekly reports of massive privacy breaches of electronic information systems, the need to protect the patient's traditional right to health information privacy and to uphold standards for the ethical practice of health care could hardly be more urgent. The public's trust in government and the nation's institutions is already at an all-time low in modern history.

On January 20, President Obama stated forcefully in his inaugural address that we must chart a new course for America under which we will return to "the ideals of our forebearers," "[remain] true to our founding documents" and preserve "the God-given promise that all are equal, all are free, and all deserve a chance to pursue their full measure of happiness." Health information technology legislation that does not recognize and protect the patient's right to health information privacy is not consistent with this new course for America.

Congress found in enacting the Privacy Act of 1974 that "the right to [informational] privacy is a personal and fundamental right protected by the Constitution of the United States" and that "the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information."¹ If we are to have a federally sponsored national electronic health information system that is consistent with the course charted by President Obama, it must contain the fundamental right to health information privacy.

¹ Pub. L. 93-579, sec. 2(a)(2), (4).

To paraphrase Reverend Martin Luther King, we should ensure that Americans are judged by the content of their character and not by the content of their health record.

We look to the Judiciary Committee to preserve and protect American's fundamental right to health information privacy.

James C. Pyles
On behalf of the American
Psychoanalytic Association

Powers, Pyles, Sutter & Verville, P.C.
1501 M Street, NW
Washington, D.C. 20005
(202) 466-6550
jim.pyles@ppsv.com

MYTHS, FACTS AND LAW ABOUT
HEALTH IT
AND THE RIGHT TO HEALTH INFORMATION PRIVACY
Revised January 27, 2008

The American Psychoanalytic Association, one of the nation's oldest and most respected mental health professional associations, offers these Myths and Facts About Health Information Technology and the Right to Health Information Privacy to the Obama Administration and the 111th Congress in the interest of (1) preserving access to effective mental health care, (2) protecting one of Americans' most cherished and fundamental rights, and (3) creating the trust that many, including the Clinton and Bush Administrations, now consider to be essential for public acceptance of a national electronic health information system.

In offering these carefully substantiated facts and law, APsaA hopes to assist the Obama Administration in abandoning the "truly poisonous legacy of the past eight years"¹ in which facts and law that were inconvenient to corporate special interests were ignored, distorted and suppressed. This is the third update of this document and, as in the past, each statement of fact and law is carefully corroborated to distinguish these "Myths and Facts" from those that may have been disseminated by other groups supported by large corporate "stakeholders" that disguise essentially unsupported personal opinion as "facts". These facts and law are offered in the hope that the Obama Administration and the new Congress will take a "reality-based" approach to the design and implementation of health IT legislation that gives priority to the interests of the one group of "stakeholders" whose support, trust and confidence is indispensable to the health care system and successful implementation of health IT—the patients.

In considering these myths and facts and legislative options, we suggest that Congress and the Obama Administration continuously ask two simple questions—(1) what would we, as patients want and (2) can any impartial person seriously believe that most Americans would be willing to relinquish their right to health information privacy in order to have access to an electronic health information system? Of course, this is a false choice since it should be possible to design a health IT system that preserves the patient's right to privacy rather than eliminates it.

1. Myth—A right to health information privacy in health IT legislation would be a new concept.

Fact—Congress has expressly found that Americans have a right to privacy for personal information about themselves that is a "personal and fundamental right protected by the Constitution of the United States".² The

¹ Bring On the Reality-Based Community, Newsweek, p. 36 (Nov. 17, 2008).

² Pub. L. 93-579, section 2(a)(4).

right to privacy in this country is “older than the Bill of Rights”.³ This “reasonable expectation” of privacy for health information has been recognized repeatedly by courts at every level of the federal judiciary.⁴ In fact, the right to privacy for highly personal health information is now so well established that no reasonable government official could be unaware of it.⁵

The right to health information privacy is also found in the physician-patient privilege recognized in 43 states⁶, and in the psychotherapist-patient privilege recognized in all 50 states and the District of Columbia and in Federal common law.⁷ The Department of Health and Human Services (HHS) has acknowledged that the privacy of highly personal information “is a fundamental right.”⁸

The right to privacy of personal information including health information is recognized under the tort law or statutory law of all 50 states.⁹ Ten states (Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington) include a specific right to privacy in their state constitutions. The Supreme Courts in other states such as Tennessee and Texas, have found that a right to privacy is implied in the state constitution.¹⁰ The standards of medical and professional ethics adopted by virtually all segments of the medical and mental health profession recognize and protect the patient’s right to health information privacy.¹¹ The Supreme Court of New Jersey has recently recognized that individuals have a right to privacy for information transmitted over the internet.¹²

The National Committee on Vital and Health Statistics (NCVHS) has found: “Privacy and confidentiality are neither new concepts, nor absolutes. Since the time of Hippocrates physicians have pledged to maintain the secrecy of information they learn about their patients

³ Griswold v. Connecticut, 381 U.S. 479, 516 (1987).

⁴ Ferguson v. City of Charleston, 532 U.S. 67 (2001); Whalen v. Roe, 429 U.S. 589 (1977); U.S. v. Scott, 424 F.3d 888 (9th Cir. 2005); Douglas v. Dobbs, 419 F.3d 1097 (10th Cir. 2005); Tucson Woman’s Clinic v. Eden, 371 F.3d 1173 (9th Cir. 2004).

⁵ Gruenke v. Seip, 225 F.3d 290, 302-03 (3rd Cir. 2000). See also, Sterling v. Borough of Minersville, 232 F.3d 190, 198 (3rd Cir. 2000).

⁶ See, e.g., Northwest Mem. Hosp. v. Ashcroft, 362 F.3d 923 (7th Cir. 2004).

⁷ Jaffee v. Redmond, 116 S.Ct. 1923 (1996).

⁸ 65 Fed. Reg. at 82,464.

⁹ HHS Finding, 65 F.R. 82,464 (Dec. 28, 2000).

¹⁰ Planned Parenthood of Middle Tenn. v. Sundquist, 38 S.W.3d 1, 6, n. 3 (Tenn. 2000).

¹¹ See, e.g., Principles of Medical Ethics, American Medical Association, “Our AMA policy is that where possible, informed consent should be obtained before personally identifiable health information is used for any purpose.” H-315.978 Privacy and Confidentiality. See also attached ethics standards.

¹² “New Jersey Justices Call E-Privacy Surfers’ Right: Ruling on Warrant Trumps Top U.S. Court’s Decisions”, The Star-Ledger (April 22, 2008).

disclosing information only with the authorization of the patient or when necessary to protect an overriding public interest, such as public health. Comparable provisions are now contained in the codes of ethics of virtually all health professionals."¹³

2. Myth—The right to health information privacy is not important for quality health care.

Fact—HHS has found that “the entire health care system is built upon the willingness of individuals to share the most intimate details of their lives with their health care providers.”¹⁴ If the privacy of sensitive health information is not recognized and protected, the information will simply not exist because the patients will not disclose it to their practitioners.¹⁵ So, “privacy is necessary to secure effective high quality health care.”¹⁶

3. Myth—An “interoperable” electronic health information system poses no new or additional threat to health information privacy.

Fact—The use of interoperable electronic health information systems for transmitting and storing identifiable health information creates the following threats to health information privacy that are unprecedented in the history of medicine:

- A. The identifiable health information of millions of individuals can be improperly disclosed to other individuals “in a matter of seconds”¹⁷;
- B. Health information may be stolen by individuals who do not have physical access to the records and who may not even reside in the United States¹⁸; and
- C. When an individual’s health information privacy is breached electronically, it can never be restored.¹⁹

¹³ Finding of the National Committee on Vital and Health Statistics, letter to Secretary Leavitt, p. 3 (June 22, 2006).

¹⁴ HHS Finding, 65 Fed. Reg. at 82,467.

¹⁵ HHS Finding, 65 Fed. Reg. at 82,468; *Jaffee v. Redmond*, 116 S.Ct. 1923, 1929 (1996).

¹⁶ HHS Finding, 65 Fed. Reg. at 82,467.

¹⁷ HHS Finding, 65 Fed. Reg. at 82,465; “An Ominous Milestone: 100 Million Data Leaks,” *The New York Times* (Dec. 18, 2006); “Vast Data Cache About Veterans is Stolen,” *The New York Times* (May 23, 2006); “Veterans Administration Loses Data,” *Consumer Affairs* Feb. 18, 2007); “Medicare and Medicaid Gaps Are Found,” *The New York Times* (Oct. 21, 2006).

¹⁸ “Experts: Medical Identity Theft Growing, Tough to Detect”, *Philadelphia Business Journal* (Oct. 19, 2007); “Breaking the Code: How Credit-Card Data Went Out Wireless Door,” *Wall Street Journal* (May 4, 2007); “Medical Identity Theft is a Growing Problem”, *The Heartland Institute* (Sept. 2007).

¹⁹ HHS Finding, 65 Fed. Reg. at 82,465.

In fact, Congress has found “the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information.”²⁰ More recently, the increasing risk to health information privacy posed by electronic information systems has been recognized by a Presidential Task Force, and the Government Accountability Office.²¹

The privacy of **at least 236 million electronic records** has been reported violated or compromised since January 1, 2005. The privacy of **at least 42,046,667 electronic health records** has been reported breached or compromised over that period of time.²² The actual number of electronic health records whose privacy has been breached or compromised could be double that number since a recent survey showed that nearly half of such breaches are not reported, and the HIPAA Privacy Rule does not require breaches to be reported.²³

4. Myth—Electronic health information systems are secure.

Fact—A recent industry sponsored survey showed that all of the electronic health information systems currently in use are “severely at risk of being hacked.”²⁴ A Presidential Cybersecurity Task Force has determined that attacks and vulnerabilities on electronic information systems are growing by 20% a year and cannot be addressed by the current “patching” approach.²⁵ HHS has found that “[T]here is no such thing as a totally secure [HIT] system that carries no risks to security.”²⁶ The Office of Management and Budget has found that **the number of attacks on federal electronic information systems increased 60% between 2006 and 2007.**²⁷

²⁰ Pub. L. 93-579, section 2(2).

²¹ “Cyber Security: A Crisis in Prioritization,” President’s Information Technology Committee, p. 5 (Feb. 28, 2005) (“The IT Infrastructure of the United States is highly vulnerable to terrorist and criminal attacks.”); “Health Information Technology: Early Efforts Initiated But Comprehensive Privacy Approach Needed for National Strategy,” GAO-07-238, p. 27 (Jan. 10, 2007) (“[T]he increased risk of inappropriate access and disclosure raises the level of importance for adequate privacy protections and security mechanisms to be implemented in health information exchange systems.”).

²² Privacy Rights Clearinghouse, <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.

²³ “Nearly Half of Data Breaches Not Disclosed: Report,” Modern Healthcare Online (April 8, 2008); 45 C.F.R. 164.530.

²⁴ “Electronic Records at Risk of Being Hacked, Report Warns,” SearchCIO.com (Sept. 19 2007).

²⁵ “Cyber Security: A Crisis in Prioritization,” *supra* at 10-12.

²⁶ HHS Finding, Security Rule, 68 Fed. Reg. at 8346 (Feb. 20, 2003).

²⁷ “Feds Losing War On Information Security, Senators Told,” Govexec.com (March 13, 2008) http://www.govexec.com/story_page.cfm?articleid=39518&den=e_gvet

5. Myth—Protection of the individual's right to health information privacy is not essential for public acceptance of a national electronic health information system.

Fact—NCVHS has determined that: "In an age in which electronic transactions are increasingly common and security lapses are widely reported, public support for the NHIN [national health information network] depends on public confidence and trust that personal health information is protected. Any system of personal health information collection, storage, retrieval, use, and dissemination requires the utmost trust of the public. **The health care industry must commit to incorporating privacy and confidentiality protections so that they permeate the entire health records system.**"²⁸

According to HHS: "Unless public fears are allayed, we will be unable to obtain the full benefits of electronic technologies. The absence of national standards for the confidentiality of health information has made the health care industry and the population in general uncomfortable about this primarily financially-driven expansion in the use of electronic data."²⁹

Even the Bush Administration has finally recognized: "The growing computerization, exchange and analysis of patient data offer the potential to improve the quality of care and reduce costs and medical errors, but those benefits won't be fully realized until privacy concerns are effectively addressed."³⁰

6. Myth—The public is not concerned about the threat that an electronic health information system poses to health information privacy.

Fact—The Government Accountability Office (GAO) has found that "... 70 percent of Americans are concerned that an electronic medical record system could lead to sensitive medical information being exposed because of weak security, and 69 percent are concerned that such a system would lead to more personal health information being shared without the patient's knowledge."³¹

7. Myth—The right to health information privacy means protecting identifiable health information from theft or improper disclosure.

²⁸ Finding of the National Committee on Vital and Health Statistics, letter to HHS Secretary Leavitt, p. 3 (June 22, 2006).

²⁹ HHS Finding, 65 Fed. Reg. at 82,466.

³⁰ Statement of HHS Secretary Michael Leavitt, HHS News (Dec. 15, 2008).

³¹ GAO Finding, "Health Information Technology, *supra* note 21, at 9-10.

Fact—NCVHS has determined that health information privacy means “an individual’s right to control the acquisition, uses, or disclosures of his or her identifiable health data.” Confidentiality means “the obligations of those who receive information to respect the privacy interests of those to whom the data relate.” Security means the “physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure.”³² According to HHS, “the right of privacy is: ‘the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated.’”³³ The courts have defined privacy as “control over knowledge about one’s self.”³⁴ And the most often quoted definition is that privacy is “the right to be let alone.”³⁵ So the accepted definition of health information privacy includes the individual’s right to control the disclosure of his or her health information.

8. Myth—The right to health information privacy is recognized and protected in the HIPAA Health Information Privacy Rule.

Fact—Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires the Secretary of HHS to set forth in regulation “the rights that an individual who is the subject of individually identifiable health information should have.”³⁶ However, **the right to health information privacy is not among the “individual rights” recognized by the Rule.**³⁷

The Original HIPAA Health Information Privacy Rule implicitly recognized the individual’s right to health information privacy by requiring consent for the use and disclosure of identifiable health information in routine situations broadly defined as treatment, payment and health care operations.³⁸ However, in 2002, that implicit right was eliminated and “replaced” by federal “regulatory permission” for all covered entities to use and disclose any individual’s identifiable health information for the same broadly defined purposes of treatment, payment and health care operations.³⁹ The HIPAA Health Information “Privacy” Rule was thereby converted from a rule that guaranteed a broad right to health information privacy to one that broadly eliminated that right.

³² Definitions adopted by the National Committee on Vital and Health Statistics from the Institutes of Medicine, letter to HHS Secretary Leavitt, p. 2 (June 22, 2006).

³³ HHS Finding quoting “Who Knows: Safeguarding Your Privacy in a Networked World”, A. Cavourkian, D. Tabscott, Random House (1995), 65 Fed. Reg. at 82,465.

³⁴ *U.S. v. Westinghouse*, 638 F.2d 570, 577, n. 5 (3rd Cir. 1980).

³⁵ “The Right to Privacy,” L. Brandeis and S. Warren, 4 Harv. L. Rev. 193 (1890)

³⁶ 42 U.S.C. 1320d-2 note.

³⁷ 45 C.F.R. §164.520(b)(1)(iv).

³⁸ 45 C.F.R. §164.506, 65 Fed. Reg. at 82,810 (Dec. 28, 2000).

³⁹ 45 C.F.R. §164.506(a), 67 Fed. Reg. at 53,211 (Aug. 14, 2002).

9. Myth—HIT legislation, even without protections for the right to health information privacy, is necessary to save 98,000 lives annually and avoid suffering due to medical errors.

Fact—The lack of adequate privacy protections in a national health IT system could well cause more deaths and injuries than it would prevent. According to HHS, nearly **600,000 Americans each year do not seek earlier treatment for cancer** due to privacy concerns.⁴⁰ As a result of these concerns, cancer victims “may ultimately face a more severe illness and/or premature death.” This delay in seeking cancer treatment costs the country an estimated **\$1.6 billion each year**. Increasing the confidence of individuals in the privacy of their medical information “would encourage more people with cancer to seek cancer treatment earlier, which would increase cancer survival rates”.

HHS has further found that more than **2 million Americans each year fail to seek treatment for mental illness** due to privacy fears.⁴¹ This untreated mental illness **costs the nation between approximately \$500 million and \$800 million each year**. Adequate privacy protections would reduce the suffering and loss associated with untreated mental illness.

HHS has also found that many Americans do not report or seek treatment for **sexually transmitted diseases** due to privacy concerns.⁴² Failure to treat sexually transmitted diseases can result in “expensive fertility problems, fetal blindness, ectopic pregnancies, and other reproductive complications.” In addition, earlier treatment “translates into reduced spread of infections.” The Centers for Disease Control and Prevention has recently found that 1 out of 4 teenage girls in America suffer from a sexually transmitted disease.⁴³

HHS has also concluded that the adverse impact of privacy concerns on the treatment of the above diseases would likely occur with “**any health condition, including relatively minor conditions**.” HHS also concluded that “some individuals might be concerned with maintaining privacy even if they have no significant health problems because it is likely that they will develop a medical condition in the future that they will want to keep private.”⁴⁴

A recent report by the RAND Corporation (the same organization that conducted in initial study on the benefits of health IT) found that **300,000 soldiers returning from the wars in Iraq and Afghanistan suffer from**

⁴⁰ 65 Fed. Reg. at 82,777.

⁴¹ 65 Fed. Reg. at 82,779.

⁴² 65 Fed. Reg. at 82,778.

⁴³ “1 in 4 Teen Girls Has At Least One STD”, Associated Press (March 11, 2008).

⁴⁴ 65 Fed. Reg. at 82,777.

Post-Traumatic Stress Disorder (PTSD) but less than half seek treatment for the reason that "if they received treatment, it would not be kept confidential and would constrain future job assignments and career advancement."⁴⁵ A "key finding" of the RAND Corp. report was that "[m]any of the most commonly identified barriers to getting needed mental health treatment could be **reduced if service members had access to confidential treatment.**"⁴⁶ **The cost of the avoidance of such is estimated to range from \$4 billion to \$6 billion** "depending on how we account for the costs of the lives lost to suicide."⁴⁷

So the failure to include privacy protections in health IT legislation is likely to exact a cost in lost lives and unnecessary suffering that is much higher than any potential savings accruing from health IT.

Further, the extent to which health IT will reduce medical errors and save lives is unclear. First, the 98,000 avoidable deaths attributed to medical errors is based on an Institutes of Medicine report in 2000 of studies in two hospitals, one in 1984 and one in 1992. The IOM report actually projected a range of possible preventable deaths ranging from 44,000 to 98,000. There has been significant question concerning whether the medical errors were actually "preventable" and whether the preventable errors actually led to the deaths of the patients.⁴⁸ For example, one recent review of the IOM study reached the following conclusion:

"The principal argument for the push to adopt CPOE has been the promise of lifesaving benefits. While we believe that CPOE has great potential to improve the health care process, we have to agree with Berger and Kichak's position that **a convincing case for lifesaving benefits has not been made.** As Berger and Kichak point out, the keystone for these arguments—namely the Institute of Medicine's (IOM's) claim of 44,000 top 98,000 deaths due to medical errors—**crumbles on close inspection.**"⁴⁹

The IOM study ignored the fact that **"the patients with adverse events had a death rate no different than the death rate (13.8%) of the target population from which they were drawn."**⁵⁰

⁴⁵ "Invisible Wounds of War", The RAND Corp., p. 436 (2008).

⁴⁶ RAND Corp. report at 436.

⁴⁷ RAND report at 438.

⁴⁸ "How Many Deaths Are Due to Medical Error? Getting the Number Right," Effective Clinical Practice (Nov./Dec. 2000) ("...Americans do not have a credible estimate of the number of deaths caused by medical error. Without such an estimate, it is impossible to make an informed policy decision about how many of our limited resources should be devoted to reducing errors as opposed to other competing health needs.")

⁴⁹ "Physicians, Information Technology, and Health Care Systems: A Journey, Not a Destination," C. Clement, M.D., et al., J. Am. Med. Inform. Assoc., 11:121-124 (March/April 2004).

⁵⁰ *Id.*

There must further be a question of how many, if any, of these medical errors even if they led to the death of the patients in 1984 and 1992 could have been prevented by an electronic health information system. The IOM study does not address that.

Recent studies have shown that electronic health information systems may add other errors.⁵¹ And some recent studies have simply not shown that electronic medical records inevitably produce higher quality care.⁵² The potential benefits of a health IT system simply do not warrant implementing such a system without the privacy protections that the history of medicine shows is essential for quality health care.

For more information, contact:

Jim Pyles, Counsel
American Psychoanalytic Association

Powers, Pyles Sutter & Verville, P.C.
1501 M Street, NW
Washington, D.C. 20005
(202) 466-6550
jim.pyles@ppsv.com

⁵¹ "Veterans Exposed to Incorrect Drug Doses," Associated Press (Jan. 14, 2009); "Not Quite Fail Safe: Computerizing Isn't a Panacea for Dangerous Drug Errors, Study Shows," The Washington Post (March 22, 2005)

⁵² "Electronic Medical Records and Diabetes Quality of Care: Results From a Sample of Family Medicine Practices," *Annals of Family Medicine* (May/June 2007) (Practices using EMRs produced worse results in care of diabetes patients.)

COALITION FOR PATIENT PRIVACY

“A.C.T.” for Privacy in 2009

January 14, 2009

Honorable Nancy Pelosi
 Speaker of the House
 United States House of Representatives
 H-232, US Capitol
 Washington, DC 20515

Honorable Harry Reid
 Senate Majority Leader
 United States Senate
 522 Hart Senate Office Bldg
 Washington, DC 20510

Dear Speaker Pelosi and Senator Reid:

Our bi-partisan Coalition, representing millions of Americans, urges you to ensure that we develop a health IT system that protects our health, jobs and privacy. We welcome the renewed commitment in Congress to protecting consumers over special interests. Consumer trust is essential to health IT adoption and participation, and only attainable with privacy.

In order to achieve a successfully wired health care system that Americans trust, we ask you, as a member of Congress, to “A.C.T.” now to ensure our information is only used to promote health:

ACCOUNTABILITY – Hold every entity with access to health information accountable.

We have learned the painful lessons of letting industry set its own rules. Consumers no longer trust that corporations will use personal health information only as directed or guard it from theft or loss.

- Those who collect, store or use personal health information should help ensure that the data is accurate, reliable and secure. Minimum standards should include: encrypting data at rest and in transit, limiting access to specific individuals via informed, electronic consent and audit trails of all electronic transactions.
- Authorize and fund Health & Human Services and the Federal Trade Commission to increase their oversight of industry practices including random audits of contracts.
- Require breach notification, privacy safeguards and whistleblower protections, including meaningful enforcement of privacy rights.

CONTROL – Ensure individuals control the use of their personal health information.

Fundamental to the Code of Fair Information Practices and most professional Codes of Ethics is an individual's right to control how their personal information is used.

- Codify a federal right to health information privacy.
- Ensure individuals can segment sensitive information and that safeguards for medical information are built in up front before problems arise.
- Provide incentives for health IT systems to use electronic informed consent, innovative consumer privacy controls and for user interfaces to be accessible for patients with disabilities.

TRANSPARENCY – Protect consumers from abusive practices.

Personal health information should not be sold and shared as a typical commodity. Health information is different; it is extremely sensitive and can directly impact jobs, credit, and insurance coverage. Commercial transfers undermine routine privacy safeguards, including transparency and accountability.

- Prohibit direct or indirect remuneration for the sharing, disclosure or use of personal health information with limited exceptions for research and public health.
- Ensure that corporations cannot obtain exclusive or contractual rights to own or control personal health information. We have evidence that selling of this data is happening at major companies (details available upon request).
- Personal health information obtained for one purpose must not be used for other purposes without informed consent. Even when consent is obtained, privacy obligations such as security and prevention of misuse, continue.

Progress for health IT and privacy is being made! We hope you will join our Coalition in protecting the right to privacy for consumers, employees, and providers.

Sincerely,

The Coalition for Patient Privacy: [Signing Organizations on following page]

cc: Members of the U.S. House of Representatives
Members of the U.S. Senate

For more information please contact:

Ashley Katz
akatz@patientprivacyrights.org
(O) (512) 732-0033
(M) (512) 897-6390

AIDS Action Council www.aidsaction.org	JustHealth www.justhealthnow.org
Alliance for Patient Safety www.allianceforpatientsafety.org	Justice Through Music www.jttmp.org
American Association for People with Disabilities www.aapd.org	Liberty Coalition www.libertycoalition.net
American Civil Liberties Union www.aclu.org	Microsoft Corporation, Inc. www.microsoft.com
Arizona Eagle Forum	The Multiracial Activist www.multiracial.com
Bazelton Center for Mental Health Law	Representative Elliot Naishtat (TX)
Bill of Rights Defense Committee www.bordc.org	National Association of Social Workers www.socialworkers.org
Citizens for Health www.citizens.org	National Center for Transgender Equality www.NCTEquality.org
Citizen Outreach Project	The National Coalition for Mental Health Professionals and Consumers www.thenationalcoalition.org
Clinical Social Work Association www.clinicalsocialworkassociation.org	National Workrights Institute www.workrights.org
Confederation of Independent Psychoanalytic Societies www.cipsusa.org	Senator Marc Pacheco (MA)
Consumer Action www.consumer-action.org	Patient Privacy Rights www.patientprivacyrights.org
Cyber Privacy Project	Private Citizen, Inc. www.privatecitizen.com
Esther Dyson www.edventure.com	Representative Cindy Rosenwald (NH)
Electronic Privacy Information Center www.epic.org	Bruce Schneier www.schneier.com
Fairfax County Privacy Council www.fairfaxcountyprivacycouncil.org	Thoughtful House Center for Children www.thoughtfulhouse.org
Government Accountability Project www.whistleblower.org	Tolven www.tolven.org
Health Administration Responsibility Project, Inc. www.harp.org	U.S. Bill of Rights Foundation
International Association of Whistleblowers www.internationalassociationofwhistleblowers.net	Velvet Revolution www.velvetrevolution.us
Senator Karen Johnson (AZ)	

Mr. Chairman, Members of the Committee:

Thank you for inviting me to testify today. Consumers Union is the independent, nonprofit publisher of *Consumer Reports*, and we work on a wide range of health issues, including prescription drug safety and effectiveness, access to health insurance and controlling health care costs.

The Potential

There's widespread agreement on the need to accelerate the use of information technology in our otherwise high-tech health-care system.¹ Most hospitals and doctor's offices still store patient records on paper, making the history of medical care hard to transfer from one hospital or doctor to another.² The inefficiencies of this system can lead to medical errors and the loss or misplacement of vital information.³ As for patients, we rarely see our own fragmented records or track our own health histories.⁴

Consumers Union therefore strongly supports the movement toward an electronic system of health records (EHR) and information exchange. By harnessing the power of modern information technology systems we can improve the quality of American health care and moderate health costs by:

- Reducing errors,
- Eliminating service duplication,
- Promoting pay for performance, and
- Providing the data necessary to evaluate the actual comparative effectiveness of various treatments and drugs.

A national system of electronic medical records has the potential to improve the quality of health care by reducing hospital-acquired infection rates. Through a network of electronic medical information, families can identify the safest and highest quality hospitals. As just one example of the tremendous improvements in quality and cost savings that are possible, Consumers Union has been conducting a national campaign to promote the disclosure of hospital infection rates (www.StopHospitalInfections.org)⁵

Each year, there are about 2 million patients who acquire infections in hospitals, and about 90,000 die. In twenty-four states, we have worked with state legislatures to pass laws to require hospitals to report their rate of infection based on the idea that public disclosure will prompt hospitals to adopt effective methods to reduce their infection rates. Electronic medical records technology and the public disclosure of more types of patient

¹ Jim Guest, President and CEO of Consumers Union, "Have You Heard: Your Medical Data, In Bits and Bytes," *Consumer Reports*, March 2006, p. 5.

² *Ibid.*

³ *Ibid.*

⁴ *Ibid.*

⁵ William Vaughan, Consumers Union --- Nonprofit Publisher of *Consumer Reports*, March 16, 2006 Testimony before the Subcommittee on Health, Committee on Energy and Commerce, U.S. House of Representatives.

care data where the patient is not identified --- will make it easier for consumers to reward those who provide quality.

The Critical Need to Ensure Privacy

While there can be important public and private benefits of creating an effective electronic medical records system, we believe (and polls demonstrate⁶) that the American public will not support, fully use, or benefit⁷ from the great potential of such systems unless more is done **now** to ensure the privacy, security, and appropriate use of medical information. In short, this requires enabling patients to decide when, with whom, and to what extent their medical information is shared.

⁸ It is important that we all recognize that there is no hack-proof database or system. Once more medical data is moving electronically, it is subject to threats from hackers, identity thieves and others. That is simply a fact of life, re-confirmed almost daily by new stories of financial and medical record data violations.⁹ Beyond the likely scenarios of security breaches, the value of electronic health information is such that many organizations will want to exploit secondary data sources for private financial gain, rarely (if ever) with patient knowledge, let alone consent. It is imperative that policy makers take aggressive steps to protect privacy. Otherwise, security breaches could doom expanded use of health information technology.

Additionally, some will say that it is too complex or too expensive to allow people to control their medical information. Computers have the ability to handle the task. They can be designed to deal with huge numbers of variables—like 50 state laws—and to create special files where certain data (such as mental health records) are only available to a designated provider on a “need to know basis.” If we do not meaningfully address the privacy issue, polls show the public will not trust this system, many will go to “off the grid” medical care,¹⁰ and we will just increase public cynicism about big government and big business controlling our lives. In an age when the talk is of consumer driven health

⁶ See as just one example Alan F. Westin, “Americans Overwhelming Believe Electronic Personal Health Records Could Improve Their Health – Nearly 9 in 10 Say Privacy Practices Are a Factor in Their Decision to Sign Up for One,” Markle Foundation – Connecting for Health, June 2008

⁷ For example, polling of Americans shows 63% to 75% would not participate in, or are concerned about loss of medical privacy in an electronic system. See work of Professor Alan Westin, February 23, 2005; California Health Care Foundation, January 2000; and 65 Federal Registrar 82,466.

⁸ Testimony of Joy Pitts, Assistant Research Professor, Georgetown University, July 27, 2005 before the Ways and Means Health Subcommittee, citing the Rep. Velasquez and former President Clinton examples, page 2. See also Robert Dallek’s *An Unfinished Life* (p261 ff) for a description of LBJ’s effort to obtain medical information on JFK and how Kennedy avoided certain medical tests so as not to have a medical record.

⁹ As HHS said in the Federal Register, “there is no such thing as a totally secure [electronic information] system that carries no risk.” 68 Federal Register at 8,346. For very recent examples of hacking and intentional misuse of data, see Information Week, March 9, 2006, “PIN Scandal “Worst Hack Ever; Citibank Only the Start,” and *The Washington Post*, March 14, 2006, Business Section, page 2, “Datran Media Settles Probe.”

¹⁰ Joy Pitts, op.cit., p.4.

care and ownership and empowerment, forcing people to share their most secret personal medical information is not the path to take.

Eroding Consumer Confidence

The inability of federal and state privacy laws to ensure the confidentiality of personal medical records continues to create grave concerns for consumers. This lack of confidence is reflected in a recent survey sponsored by the Institute of Medicine Project on "Health Research, Privacy, and the HIPAA Privacy Rule." The survey found that 58 percent of respondents believe that the privacy of personal medical records and health information is not protected well enough today by federal and state laws and organizational practices.¹¹ Nonetheless, the public appears to recognize that electronic health records offer the potential of enormous gains for consumers and society in improved health outcomes and cost savings. In a recent survey by the Markle Foundation, two in three Americans (65 percent) would like to access all of their own medical information across an electronic network.¹² Americans believe that having greater access to their information will reduce medical mistakes and costly repeat procedures. According to this Markle Foundation survey, 96 percent of respondents stated that they thought it was important for individuals to be able to access all their own medical records to manage their own health.¹³ At the same time, such a system raises serious concerns among consumers about personal privacy, data security, and the potential misuse of their information.¹⁴ And while an interoperable system of electronic health information holds great promise, the many possible benefits will not be realized unless appropriate policy measures to protect personal medical information are established up front.¹⁵

Better Understanding of Existing Rights

Consumers struggle with a lack of understanding about their rights stemming from existing medical privacy protections. For example, a national consumer health privacy survey found that consumers are unfamiliar with medical privacy protections.¹⁶ In this survey, two-thirds of the survey respondents stated that they were aware of federal protections for their personal medical records, and 59 percent recall receiving a privacy notice but only 27 percent believe they have more rights than they had before receiving the notice.¹⁷ Simply put, the growing evidence of confusion must commit us to better educating the public, not to undermining support for the medical privacy protections for

¹¹ Dr. Alan F. Westin, Professor of Public Law and Government Emeritus, Columbia University, Director, Health Privacy Program, Privacy Consulting Group at the Institute of Medicine Workshop on "How the Public Sees Health Research and Privacy Issues," Washington, DC, February 28, 2008.

¹² Markle Foundation, "Americans See Access to Their Medical Information as a Way to Improve Quality, Reduce Health Care Costs," December 7, 2006, p. 1.

¹³ *Ibid.*

¹⁴ Consumer Partnership for e-Health, Letter to the Honorable Patrick J. Leahy, Chairman, Committee on Judiciary, U.S. Senate, May 15, 2008.

¹⁵ *Ibid.*

¹⁶ California HealthCare Foundation, "National Consumer Health Privacy Survey," November 2005.

¹⁷ *Ibid.*

which the public clamored for decades.¹⁸ In keeping with this effort to better inform the public, Consumers Union has used our publication *Consumer Reports* to inform our 8 million subscribers about their rights, as well as encourage others to visit the Health Privacy Project website which has merged with Center for Democracy and Technology to download their user-friendly brochure “Know Your Rights.”

When consumers are confused, they are fearful that there is widespread misuse of personal medical information. This concern regarding the privacy of their medical information manifests itself in consumers engaging in “off the grid” medical care. These privacy-protective behaviors include patients providing false or incomplete information to physicians, doctors inaccurately coding files or leaving certain things out of a patient’s record, people paying out of pocket to avoid a claim being submitted, or in the worst cases, people avoiding care altogether.¹⁹ Therefore, it is critical that consumers have a full understanding of their medical privacy rights and confidence in the federal health privacy law to preserve the confidentiality of their medical records. Otherwise, people are forced to choose between shielding themselves from discrimination and receiving health care services.

Conclusion

Thus, Consumers Union along with members of the Consumer Partnership for e-Health, a non-partisan group of consumer, labor, patient, and research organizations is dedicated to broadening access to health care, and improving the quality of care by ensuring that consumer’s medical information is safeguarded in the health care arena. We believe that health information technology and exchange (HIT/HIE) are critical underpinnings of a more patient-centered health care system. It can facilitate better coordination of care regardless of patient location, encourage higher quality and more efficient care, increase system transparency, and encourage patients’ active engagement in health care decision-making. However, sound policies must ensure that the systems and processes developed for the purpose of HIT/HIE enable consumer engagement and hold all those with access to personal health information accountable for how this information is handled and used.

The Consumer Partnership for e-health thus has developed a set of principles that achieve an effective balance between promoting HIT/HIE and systemic privacy safeguards. These principles are attached to my written testimony for the Committee’s review and consideration when developing legislation to address medical privacy concerns in the context of HIT.

Thank you?

¹⁸ Ibid.

¹⁹ Ibid.

Health Information Technology – Consumer Principles

March 2006

An interoperable system of electronic health information holds many potential benefits for consumers, including: better coordination of health care regardless of patient location, higher quality and more efficient care, increased system transparency, and patient access to information about providers that allows them to make better decisions. At the same time, such a system raises serious concerns among consumers about personal privacy, data security, and the potential misuse of their information. And while an interoperable system of electronic health information holds great promise, the many possible benefits will not be realized unless appropriate policy measures are established up front.

Consumer protections and potential benefits from health information technology (HIT) should not be left to chance. The success of efforts to promote widespread adoption of HIT, including electronic connectivity and data exchange across health care institutions, ultimately will depend on the willingness of consumers to accept the technology. Given the pervasive concerns expressed by the public about unauthorized disclosure and use of their health information, it is critical to build a foundation of public trust. To that end, as efforts move forward to develop networks for the electronic exchange of information between institutions, there must be a clear, deliberate, and open forum for addressing and setting matters of policy. As organizations representing a broad and diverse set of consumer interests, we believe that the following set of principles should underpin such efforts.

Principles

Individuals should be able to access their personally identifiable health information conveniently and affordably.

- Individuals should have a means of direct, secure access to their electronic health information that does not require physician or institutional mediation.
- Individuals should have access to all electronic records pertaining to themselves (except in cases of danger to the patient or another person).
- Individuals should be able to supplement, request correction of, and share their personally identifiable health information without unreasonable fees or burdensome processes.

Individuals should know how their personally identifiable health information may be used and who has access to it.

- Individuals should receive easily understood information identifying the types of entities with access to their personal health information and all the ways it may be used or shared. The explanation should include any sharing for purposes other than the immediate care of the individual, and should explicitly identify intentions for data use such as public health protection, quality improvement, prevention of medical errors, medical research or commercial purposes.

- Access to personal health information must be limited to authorized individuals or entities.
- Tracking and audit trail systems should be in place that permit individuals to review which entities have entered, accessed, modified and/or transmitted any of their personally identifiable health information.

Individuals should have control over whether and how their personally identifiable health information is shared.

- Individuals should be able to opt out of having their personally identifiable health information – in whole or in part – shared across an electronic health information network.
- Individuals should be able to limit the extent to which their health information (with or without personal identifiers) is made available for commercial purposes.
- Individuals should be able to designate someone else, such as a family member, caregiver or legal guardian, to have access to and exercise control over how records are shared, and also should be able to rescind this designation.

Systems for electronic health data exchange must protect the integrity, security, privacy and confidentiality of an individual's information.

- Personally identifiable health information should be protected by reasonable safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data. These safeguards must be developed at the front end and must follow the information as it is accessed or transferred.
- Individuals should be notified in a timely manner if their personally identifiable health information is subject to a security breach or privacy violation.
- Meaningful legal and financial remedies should exist to address any security breaches or privacy violations.
- Federal privacy standards that restrict the use and disclosure of personally identifiable health information should apply to all entities engaged in health information exchanges.

The governance and administration of electronic health information networks should be transparent, and publicly accountable.

- Independent bodies, accountable to the public, should oversee electronic health information sharing.
- Consumers should have equal footing with other stakeholders.

Recognizing the potential of electronic patient data to support quality measurement, provider and institutional performance assessment, relative effectiveness and outcomes research, prescription drug monitoring, patient safety, public health, informed decisionmaking by patients and other public interest objectives, systems should be designed to fully leverage that potential, while protecting patient privacy.

Implementation of any regional or national electronic health information network should be accompanied by a significant consumer education program so that people understand how the network will operate, what information will and will not be available on the

network, the value of the network, its privacy and security protections, how to participate in it, and the rights, benefits and remedies afforded to them. These efforts should include outreach to those without health insurance coverage.

AARP
AFL-CIO
American Federation of State, County and Municipal Employees
American Federation of Teachers
Center for Medical Consumers
Communications Workers of America
Consumers Union
Department for Professional Employees, AFL-CIO
Childbirth Connection
Health Care for All
Health Privacy Project
International Association of Machinists and Aerospace Workers
International Union, United Auto Workers
National Coalition for Cancer Survivorship
National Consumers League
National Partnership for Women & Families
Service Employees International Union
Title II Community AIDS National Network
United Steelworkers International Union (USW)

**Health Care Reform and
Personal Health Information Privacy**

Testimony to Senate Judiciary Committee
Hearing on "Health IT: Protecting Americans' Privacy in the Digital Age"
January 27, 2009

James Hester Jr. PhD
Director,
Health Care Reform Commission
Vermont State Legislature
802 828-1107
jhester@leg.state.vt.us

Health Care Reform and
Personal Health Information Privacy

Thank you for the opportunity to testify on this critical issue. I am currently the Director of the Health Care Reform Commission for the Vermont State Legislature and a member of the board of Vermont Information Technology Leaders (VITL), the state wide health information exchange network (HIEN). My testimony today does not reflect the official positions of the legislature, commission or VITL. (VITL has submitted separate written testimony.) My personal opinions have been shaped by seven years active involvement in health care reform in Vermont and thirty five years of experience in the health care industry where I have been engaged in using information and IT to improve the performance of the health care system. I come before you today not as a privacy expert or IT expert, but rather as one with extensive experience in using information and IT as a means to furthering the end of effective health care reform – making quality health care available to every resident of Vermont.

Health care reform in Vermont has been underway for almost eight years, but was first codified in Act 191 in 2006. Due to a unique combination of conditions including its size, delivery system and collaborative culture, Vermont has become a statewide laboratory for health care reform. The reform effort is the most comprehensive state reform initiative in the country, and is built on the ‘three legged stool’ of

1. **Expanding affordable coverage:** We established the goal of reducing the number of uninsured in the state from 10% in 2005 to 4% in 2010. As of October, 2008, the uninsured rate had declined to 7.6%, even in the face of a troubled economy.
2. **Bending the medical cost curve by improving the prevention and treatment of chronic illnesses:** As of March 2009, 10% of Vermont’s residents will participate in ‘enhanced pilots’ implemented by the Blueprint for Health. These pilots will combine payment reform for all payers, the use of local care teams and information tools and implementation of an integrated prevention program
3. **Using information technology as a catalyst for performance improvement:** Sustainable improvement in coverage and chronic illness care can only be achieved with the support of health information technology. We believe that it is impossible to obtain the desired performance of our health care and prevention system as long as key clinical information is only available to providers and patients through paper charts sitting in filing cabinets.

The primary vehicle for the third component of the health care reform, health information technology, has been VITL. VITL is a new public/private organization which was given the responsibility to plan and implement the statewide health IT strategy. In the last three years it has accomplished the following:

1. Completed a state Health IT plan for both the statewide health information exchange network (HIEN) and the diffusion of Electronic Medical Records (EMR's)
2. Implemented a pilot program in providing medication histories for patients in hospital emergency rooms
3. Provided support for the information tools being used in the Blueprint for Health pilot communities
4. Implemented a pilot program in assisting primary care physicians in selection, contracting, financing and implementation of EMR's
5. Contracted with GE Healthcare to provide the core infrastructure for the statewide health information exchange and begun building the interfaces to hospitals, physicians and other sources. VITL plans to launch an advanced health information exchange pilot in at least one community in 2009.
6. Planned a statewide e prescribing initiative which it hopes to begin by July, 2009

Last May, Vermont became the first state in the country to provide the long term financing to pay for the development of the statewide HIEN and for EMR's for all independent primary care practices in the state. A Health Information Technology Fund was created to raise \$32 million over the next seven years through an assessment of 0.2% on all paid claims in the state. The first payment was collected last October and VITL has begun drawing down on this fund.

This transition from creating a plan and implementing relatively small scale pilots to full scale statewide implementation has provided a major impetus for the review of the Personal Health Information privacy and security policies of VITL. The legislature has had a long standing interest in this area, as is indicated by its passing legislation requiring an active patient opt in for consent, passing major limitations and controls of data mining of prescription data, and ensuring that privacy and security standards were included as an explicit component of the state health IT plan. To address its changing needs and respond to concerns, VITL initiated a broad based stakeholder review process to update the health IT plan and revise its operating policies and procedures. Those efforts are in their final stages, but are now on hold pending clarification of the proposed privacy guidelines in the economic stimulus act (American Recovery and Reinvestment Act).

While the health IT financing implemented in Vermont's health IT fund and proposed in ARRA is extremely helpful and goes far toward reducing the financial barrier to widespread implementation of health IT, it is not sufficient by itself. Realizing the benefits of health IT requires broad acceptance by both patients and providers of this new technology which deals with the most sensitive types of data – Personal Health Information. The process that VITL has engaged in represents a delicate balancing act between sometimes conflicting interests of consumer control and needs and provider accountability and responsibilities. Unless consumers are confident that their information is secure and will be used appropriately, they will not participate in electronic health information exchanges. Unless providers believe that the administrative burdens are reasonable and the information is reliable, they will not participate in such exchanges either.

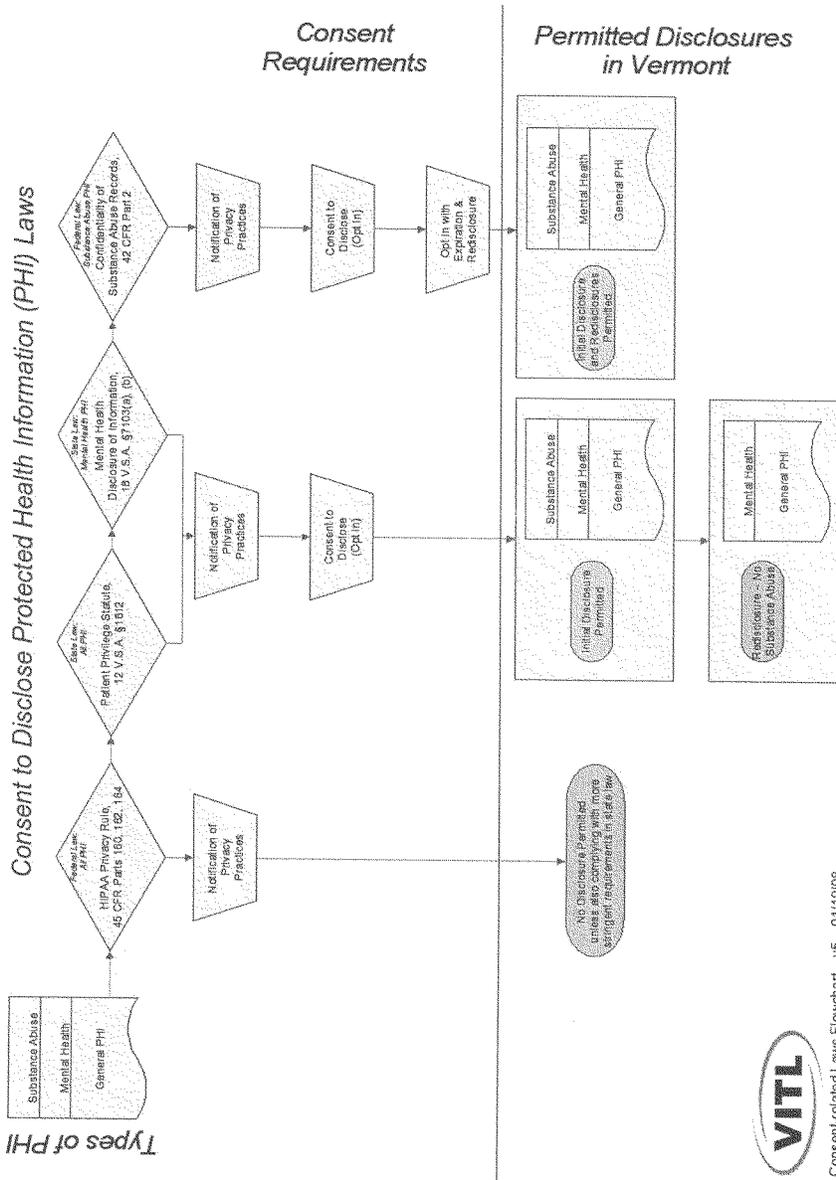
Consent policies provide an excellent case study of this balancing of interests. The attached flowchart shows the state and federal regulations governing consent of PHI in Vermont. Working within this legal framework, VITL had to resolve such questions as

- Given that state law requires that patients opt in to participate in the HIEN, should this initial consent have an expiration date? If not, should patients be periodically reminded of their ability to opt out?
- Should reauthorization to share PHI with other treating providers be required for PHI other than the legally mandated substance abuse PHI?
- What uses, if any, should require a separate consent by the patient?

Moving forward with our health care reform totally depends upon finding an initial balance point between conflicting needs and interests in a way which will encourage broad based participation of patients and providers. I am confident that once the federal privacy guidelines and requirements in the ARRA are finalized, VITL will be able to rapidly complete the revision of its guiding principles and operating policies.

However, this balance point is not static – it will evolve. We fully expect that the implementation of the initial privacy policies in a steadily growing set of pilot health reform initiatives such as the Blueprint enhanced medical home, medication history for ER patients, e prescribing and the proposed pilot community health information exchange will teach us important lessons over the next couple of years. We will have to return to the privacy policies on a regular basis to update them based what we have learned and new technical capabilities. The core security and privacy capabilities have been carefully thought through and provide a sound foundation for beginning this expansion. Experience has demonstrated that the only way to develop a high performing system is to test it through implementation combined with rapid cycle improvement. The Vermont health care reform program has been built on scalable, community level pilot programs which have enabled us to learn rapidly what works and what needs to be improved. We will use this model to evolve our privacy and security policies and capabilities as well.

Given the strong feelings surrounding Personal Health Information and the uncertainties that are inherent in the early stages of the spread of EMR's and the use of health information exchange, I fully expect that a significant minority of both patients and providers may elect not to participate. A reasonable goal is to devise a program which will satisfy the needs of a large enough percentage (60-80%?) of users to enable robust testing of capabilities, deliver value to the users and drive the next round of privacy and security technology. As capabilities mature and confidence grows, the hope and expectation is that our program will earn the trust of a steadily expanding percentage of both our population and health care delivery system. The successful scaling up of our pilot programs into system wide initiatives and the long term success of our health reform efforts depend on it.



Consent-related Laws Flowchart - v5 - 01/19/06

**TESTIMONY BEFORE THE UNITED STATES SENATE JUDICIARY COMMITTEE
ON
"HEALTH IT: PROTECTING AMERICANS' PRIVACY IN THE DIGITAL AGE"**

January 27, 2009

By John P. Houston
Vice President, Information Security and Privacy; Assistant Counsel
University of Pittsburgh Medical Center

I am grateful for the opportunity to address the Senate Judiciary Committee regarding this important topic. I would like to start by stating that the adoption of Healthcare Information Technology (Health IT) is one of the most significant healthcare initiatives that this nation can undertake. The adoption of Health IT will lead to substantial improvements in healthcare delivery, reductions in medical error rates, reductions in costs and improvements in population health, while accelerating medical research. However, the widespread adoption of Health IT will not be successful if our patients' privacy expectations are not met. The reality is that we are all patients at some point in our lives, and as such, we expect that our medical records will remain confidential. This reality drives healthcare professionals to make the appropriate decisions regarding privacy practices.

I am proud to say that UPMC has one of the most progressive and longstanding programs for the development and deployment of health IT in the world. For example:

- UPMC's new Children's Hospital will utilize an entirely electronic medical record, leaving no accommodations for paper medical records.
- UPMC's system currently has over 24,138 users, and 3,075,273 unique electronic patient records.
- Computerized Physician Order Entry (CPOE) is deployed at 46% of UPMC's inpatient units while nationally the rate is less than 2%.
- UPMC's ambulatory electronic medical record (EMR) is deployed to 60% of UPMC's 2,300 employed physicians. The national benchmark is 4%.
- UPMC has invested more than \$1 billion in information technology over the last five years to improve the quality, safety and efficiency of patient care.
- Both, UPMC Presbyterian and Children's Hospital of Pittsburgh have achieved Stage 6 of the HIMSS Analytics EMR Adoption model. This level recognizes facilities that have provided their caregivers with advanced EMR functionality that includes: ancillary systems, clinical data repository, decision support, CPOE, Positive Patient Identification and physician documentation within an integrated EMR. The average U. S. hospital is automated to the Stage 2 level.

UPMC's health system features:

- 50,000 employees

- More than \$7 billion in revenue
- 20 tertiary, specialty, and community hospitals (including a psychiatric hospital, a children's hospital, and a women's hospital)
- 400 outpatient sites and doctors' offices, with approximately 3 million patient visits per year
- Retirement and long-term care facilities
- An insurance plan that covers 1.3 million members through a variety of insurance programs

Having been accountable for both privacy and information security at UPMC for the last eight years, I believe that I have developed a deep understanding for both. I am not only aware of the public policy considerations underlying privacy and information security, but also the operational balance between a patient's right to privacy, and providing timely and complete information necessary for the delivery of effective health care. Unfortunately, this balance is neither precise nor clear. I have seen firsthand how information barriers established in the interest of privacy have detrimentally affected patient care.

I have reviewed the current draft of the privacy legislation that was included in the "Health Information Technology for Economic and Clinical Health Act" (the "Act"). While the Act attempts to address the evolving privacy and security requirements that have arisen since the implementation of HIPAA, it falls short of providing a comprehensive and workable framework. In too many cases, the Act calls for study or review. In other cases, the Act imposes obligations that are overly burdensome, while falling short of advancing privacy. I believe that we would be better served by spending additional time to develop a comprehensive and balanced privacy and security framework, than by adopting these privacy and security rules.

Regarding the privacy and security sections of the Act, I have the following comments:

Business Associates. I agree that business associates and others should be held to the same privacy and security standard as covered entities. In addition, obligating business associates to notify the covered entity of a breach further strengthens existing HIPAA requirements. However, statutory guidance is necessary regarding enforcement, and to define a covered entity's responsibilities, with regard to the act of the business associate. Without such guidance, the Act may impede the operation of business associates and covered entities.

Patient Notice of Breaches. Under HIPAA, the covered entity is required to make an accounting of disclosure in any case where an inappropriate disclosure has occurred. While the Act reasonably requires the covered entity to notify a patient of a breach of the patient's health information, in certain cases it also requires the covered entity to post breaches on its website. In other instances, the Act requires the covered entity to notify the media. Additionally, the Act calls for the reporting of all breaches to HHS.

I am concerned that there will be limited practical benefit associated with the website posting or media notice, in relation to the associated effort. Further, it would appear that the purpose of reporting breaches is punitive, rather than serving a constructive purpose.

Technology Standards. The Act provides that technologies shall be specified for securing identifiable health information. While the concept of establishing specific standards may seem appealing, technologies and security threats change on an almost daily basis. Furthermore, requirements vary greatly between covered entities, based on how they have implemented technology. Therefore, the establishment of specific standards may actually retard or prevent the adoption of appropriate security measures.

Restrictions on Certain Disclosures of Health Information. The act provides that patients have the right to restrict a health plan from gaining access to aspects of their record, related to privately paid patient services. In practice, such restrictions will be difficult, if not impossible, to administer and moreover, could deprive caregivers of vital information necessary to treat the patient appropriately.

Accounting of Disclosures. The Act provides that a patient is entitled to receive an account of whoever accessed their electronic record, even if such access was for treatment, payment or health care operations. For an inpatient encounter, it would not be uncommon for more than two-hundred people to access various aspects of a patient's record. This would include physicians, nurses, aids, dieticians, phlebotomist, social workers, physical therapists, medical records staff, coders, billing office staff and others. If a patient is provided with a listing of everyone who accessed the patient's record, the provider will then need to be prepared to explain each individual access. In practice, this could result in substantial and costly efforts on behalf of the provider with little or no apparent benefit to the patient.

Health Care Operation. The act provides that the Secretary will propose limitations on the use of identifiable health information for health care operations purposes. Currently, there are a wide variety of health care operations purposes that require the use identifiable patient information. I am unsure whether all of these purposes can be identified, let alone reasonably characterized. Further, the burden associated with de-identifying patient information must be considered, not only in terms of the time and effort associated with performing the de-identification, but also in terms of the likelihood that the covered entity will simply choose not to perform the health care operation.

Fundraising. The Act provides that fundraising would no longer be considered to be part of health care operations. The Act is unclear whether this change has the effect of eliminating the right to perform fundraising as otherwise provided for in HIPAA. In difficult economic times and an era of shrinking reimbursements, fundraising is of critical importance to most providers. Any restriction on fundraising will further frustrate providers' ability to deliver quality health care.

Personal Health Records (PHR) Providers, Health Information Exchanges, Regional Health Information Organizations and Others. The Act attempts to address PHR providers, Health Information Exchanges (HIE), Regional Health Information Organizations (RHIO) and other entities that had historically fallen outside the coverage of HIPAA. However, the Act's treatment of each is neither comprehensive nor consistent. Rather than establishing an inconsistent privacy patchwork, a single framework needs to be established to accommodate not only today's requirements, but which also can be extended to cover the rapidly evolving Health IT environment.

Enforcement. While there has been much criticism of current enforcement strategies, I believe that the manner in which enforcement is performed has been effective. Currently, covered entities can work collaboratively with the Office of Civil Rights (OCR) when privacy issues arise. For example, UPMC has performed self reporting to OCR on a number of occasions. As worded, the Act substantially increases penalties and enforcement. The Act must ensure that the opportunity to collaborate exists for those covered entities that are dedicated to protecting their patient's privacy.

Audits. The Act provides for periodic audits of covered entities and business associates. The Act should require that audit criteria be established and published, so that covered entities and business associates can engage internal and external auditors, to conduct audits that would satisfy the Act's requirement.

Studies, Reports and Guidance. The Act requires that a study be undertaken to assess the privacy and security requirements of non-HIPAA covered entities, and also requires that a report be developed regarding compliance with the Act. Further, the Act requires that guidance on de-identification of protected Health information be provided. While I agree that a study, report and guidance should be undertaken, they should be undertaken in the context of developing a comprehensive privacy and information security framework for health information. This study, report and guidance should be performed in advance of enacting legislation, rather than as a result of the Act.

Statement of Senator Patrick Leahy
Chairman, Senate Judiciary Committee
Hearing on "Health IT: Protecting Americans' Privacy in the Digital Age"
January 27, 2009

Today, the Committee holds an important hearing on how best to protect Americans' health privacy rights as the Nation moves towards a national health IT system. I have long held the view that American innovation can – and should – play a vital role in improving our Nation's health care system. That is why I am pleased that President Obama has called for the immediate investment in health information technology; so that all of America's medical records are computerized within five years.

In America today, if you have a health record, you have a health privacy problem. The explosion of electronic health records, digital databases, and the Internet is fueling a growing supply of and demand for Americans' health information.

The ability to easily access this information electronically – often by the click of a mouse, or a few key strokes on a computer – can be very useful in providing more cost-effective health care. But, the use of advancing technologies to access and share health information can also lead to a loss of personal privacy.

Without adequate safeguards to protect health privacy, many Americans will simply not seek the medical treatment that they need for fear that their sensitive health information will be disclosed without their consent. And those who do seek medical treatment assume the risk of data security breaches and other privacy violations. Likewise, health care providers who perceive the privacy risks associated with health IT systems as inconsistent with their professional obligations will avoid participating in a national health IT system.

In my state of Vermont, we have formed a public-private partnership that is charged with developing Vermont's statewide electronic health information system, including a policy on privacy. I believe that in order for a national health IT system to succeed, we in Congress should follow Vermont's good example and work together with public and private stakeholders to ensure the privacy and security of electronic health records. That is why I have worked very

hard for more than a decade with Senator Kennedy – a tireless champion of health IT – many other Members of Congress on both sides of the aisle, and numerous stakeholders in the public and private sectors, to craft bipartisan health privacy legislation. I will continue to work on this pressing issue during the 111th Congress.

Recently, some have suggested that addressing privacy in health IT legislation is too hard and that Congress should simply put off this issue for another day. But, without meaningful privacy safeguards, our Nation's health IT system will fail its citizens.

In his inaugural address, President Obama eloquently noted that in our new era of responsibility “there is nothing so satisfying to the spirit, so defining of our character than giving our all to a difficult task.” Today's hearing is an important step towards tackling the difficult, but essential task of ensuring meaningful health information privacy for all Americans.

The first hearing that I held when I resumed the Chairmanship at the start of the last Congress was a hearing on privacy and, once again, one of the Committee's first hearings for this new Congress is on privacy. We have a distinguished panel of privacy experts, government officials and consumer advocates to help us examine this issue. I thank all of our witnesses for appearing today and I look forward to a productive discussion.

#####

Statement of Deven McGraw
Director, Health Privacy Project
Center for Democracy & Technology
Before the
Senate Judiciary Committee
“Health IT: Protecting Americans’ Privacy
in the Digital Age”

January 27, 2009

Chairman Leahy and members of the Committee, thank you for holding this hearing on “Health IT: Protecting Americans’ Privacy in the Digital Age.”

CDT is a non-profit public interest organization founded in 1994 to promote democratic values and individual liberties for the digital age. CDT works to keep the Internet open, innovative and free by developing practical, real-world solutions that enhance free expression, privacy, universal access and democratic participation. The Health Privacy Project, which has more than a decade of experience in advocating for the privacy and security of health information, was merged into CDT last year to take advantage of CDT’s long history of expertise on Internet and information privacy issues. Our mission is to develop policies and practices that will better protect the privacy and security of health information on-line and build consumer trust in e-health systems.

This hearing could not be more timely or more important. Now pending before Congress is economic recovery legislation that includes \$20 - 23 billion to promote the widespread adoption of health information technology and electronic health information exchange (commonly referred to as health IT). Health IT holds enormous potential to improve health care quality and engage consumers more actively in their own healthcare, and building and implementing an electronic health information exchange infrastructure is critical to achieving the goals of health reform. Surveys consistently demonstrate the support of the American public for health IT.

At the same time, however, the public is very concerned about the risks health IT poses to health privacy. A system that makes greater volumes of information available more efficiently to improve care will be an attractive target for those

who seek personal health information for commercial gain or inappropriate purposes. Building public trust in health IT systems is critical to realizing the technology's potential benefits. Just two weeks ago, in a hearing before the Senate Finance Committee, the U.S. Government Accountability Office (GAO) stated that "a robust approach to privacy protection is essential to establish the high degree of public confidence and trust needed to encourage widespread adoption of health IT and particularly electronic medical records."

While some persist in positioning privacy as an obstacle to achieving the advances that greater use of health IT can bring, it is clear that the opposite is true: enhanced privacy and security built into health IT systems will bolster consumer trust and confidence and spur more rapid adoption of health IT and realization of its potential benefits. A commitment to spend significant federal dollars to advance health IT must be coupled with a strong commitment to enacting comprehensive privacy and security protections. Congress' role is critical here, and privacy protections must be part of any legislation that promotes electronic health records.

The privacy provisions in the proposed legislation take concrete, incremental steps toward the realization of a comprehensive framework of privacy and security protections for electronic health information, and CDT supports them. However, they are only a first step. Assuring privacy and security for electronic health information will require an ongoing commitment by Congress, the Administration, and the private sector. Congress should consider adding to the bill additional oversight and enforcement language to ensure that the stimulus funds are spent in a way that enhances rather than erodes privacy.

Why Privacy and Security Protections are Critical to Health IT

As noted above, survey data shows that Americans are well aware of both the benefits and the risks of health IT. A large majority of the public wants electronic access to their personal health information – both for themselves and for their health care providers. At the same time, people have significant concerns about the privacy of their medical records. In a 2006 survey, when Americans were asked about the benefits of and concerns about online health information:

- 80% said they are very concerned about identity theft or fraud;
- 77% reported being very concerned about their medical information being used for marketing purposes;
- 56% were concerned about employers having access to their health information; and

- 55% were concerned about insurers gaining access to this information.¹

Health IT has a greater capacity to protect sensitive personal health information than is the case now with paper records. Digital technologies, including strong user authentication and audit trails, can be employed to limit and track access to electronic health information automatically. Electronic health information networks can be designed to facilitate data sharing among health care system entities for appropriate purposes without needing to create large, centralized databases that can be vulnerable to security breaches. Encryption and similar technologies can reduce the risk to sensitive data when a system is breached. Privacy and security policies and practices are not 100% tamperproof, but the virtual locks and enforcement tools made possible by technology can make it more difficult for bad actors to access health information and help ensure that, when there is abuse, that the perpetrators will be detected and punished.

At the same time, the computerization of personal health information—in the absence of strong privacy and security safeguards—magnifies the risk to privacy. Tens of thousands of health records can be accessed or disclosed through a single breach. Headlines just last year about the theft of an NIH laptop loaded with identifiable information about clinical research subjects underscored these concerns, and that was just one of numerous examples. The cumulative effect of these reports of data breaches and inappropriate access to medical records, coupled with a lack of enforcement of existing privacy rules by federal authorities, deepens consumer distrust in the ability of electronic health information systems to provide adequate privacy and security protections.²

Protecting privacy is important not just to avoid harm, but because good health care depends on accurate and reliable information.³ Without appropriate protections for privacy and security in the healthcare system, patients will engage in “privacy-protective” behaviors to avoid having their personal health information used inappropriately.⁴ According to a recent poll, one in six adults (17%) – representing 38 million persons – say they withhold information from their health providers due to worries about how the medical data might be

¹ Study by Lake Research Partners and American Viewpoint, conducted by the Markle Foundation (November 2006) (2006 Markle Foundation Survey).

² See <http://www.cdt.org/healthprivacy/20080311/stories.pdf> for stories of health privacy breaches and inappropriate uses of personal health information.

³ See Janlori Goldman, “Protecting Privacy to Improve Health Care,” *Health Affairs* (Nov-Dec, 1998) (Protecting Privacy); Promoting Health/Protecting Privacy: A Primer, California Healthcare Foundation and Consumers Union (January 1999), <http://www.chcf.org/topics/view.cfm?itemID=12502> (Promoting Health/Protecting Privacy).

⁴ *Id.*

disclosed.⁵ Persons who report that they are in fair or poor health and racial and ethnic minorities report even higher levels of concern about the privacy of their personal medical records and are more likely than average to practice privacy-protective behaviors.⁶ The consequences of this climate of fear are significant – for the individual, for the medical community, and for public health.

It is often difficult or impossible to establish effective privacy protections retroactively, and restoring public trust that has been significantly undermined is much more difficult—and more expensive—than building it at the start. Now, in the early stages of health IT adoption, is the critical window for addressing privacy.

■ We Need a Comprehensive Privacy and Security Framework That Will Build Public Trust, Advance Health IT

To build public trust in health IT, we need the second generation of health privacy — specifically, a comprehensive, flexible privacy and security framework that sets clear parameters for access, use and disclosure of personal health information for all entities engaged in e-health. Such a framework should be based on three pillars:

- Implementation of core privacy principles;
- Adoption of trusted network design characteristics; and
- Strong oversight and accountability mechanisms.

In developing this comprehensive framework, policymakers, regulators, and developers of HIT systems need not start from scratch. A framework for HIT and health information exchange already exists, in the form of the generally accepted “fair information practices” (“FIPS”) that have been used to shape policies governing uses of personal information in a variety of contexts. While there is no single formulation of the “FIPs,” the Common Framework developed by the Markle Foundation’s multi-stakeholder Connecting for Health initiative provides a good model.⁷

Of particular relevance for this hearing, the core privacy principles of the Connecting for Health Common Framework set forth a comprehensive, flexible

⁵ Harris Interactive Poll #27, March 2007.

⁶ National Consumer Health Privacy Survey 2005, California HealthCare Foundation (November 2005).

⁷ See www.connectingforhealth.org for a more detailed description of the Common Framework.

roadmap for protecting the privacy and security of personal health information while still allowing information to be accessed and disclosed for legitimate purposes. Those core privacy principles are:

- **Openness and Transparency:** There should be a general policy of openness about developments, practices, and policies with respect to personal data. Individuals should be able to know what information exists about them, the purpose of its use, who can access and use it, and where it resides.
- **Purpose Specification and Minimization:** The purposes for which personal data is collected should be specified at the time of collection, and the subsequent use should be limited to those purposes or others that are specified on each occasion of change of purpose.
- **Collection Limitation:** Personal health information should only be collected for specified purposes, should be obtained by lawful and fair means and, where possible, with the knowledge or consent of the data subject.
- **Use Limitation:** Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.
- **Individual Participation and Control:**
 - Individuals should control access to their personal health information:
 - Individuals should be able to obtain from each entity that controls personal health data, information about whether or not the entity has data relating to them.
 - Individuals should have the right to:
 - Have personal data relating to them communicated within a reasonable time (at an affordable charge, if any), and in a form that is readily understandable;
 - Be given reasons if a request (as described above) is denied, and to be able to challenge such a denial;
 - Challenge data relating to them and have it rectified, completed, or amended.
- **Data Integrity and Quality:** All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete and current.
- **Security Safeguards and Controls:** Personal data should be protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification or disclosure.
- **Accountability and Oversight:** Entities in control of personal health data must be held accountable for implementing these information practices.
- **Remedies:** Legal and financial remedies must exist to address any security breaches or privacy violations.

The privacy and security regulations under the Health Insurance Portability and Accountability Act (HIPAA) include provisions addressing some of these principles – but, as discussed in more detail below, the HIPAA rules are insufficient to cover the new and rapidly evolving e-health environment. To get to the second generation of health privacy and build consumer trust in e-health systems, Congress should:

- Direct the Secretary of the Department of Health and Human Services (HHS) to develop policies and programs to ensure that all entities that receive federal funds for health IT adopt and implement policies and technological solutions that address each of the principles set forth above, and to hold funding recipients accountable for complying with such policies and applicable law.
- Strengthen HIPAA for records kept by traditional health system participants (i.e., physicians, hospitals, pharmacists, health plans) and fill gaps in HIPAA's rules where appropriate; and
- Establish additional legal protections to reach new actors in the e-health environment and address the increased migration of personal health information out of the traditional medical system.

Congress should set the framework for national policy through legislation, but ensuring and enforcing adequate protections for privacy and security also will require coordinated actions on the part of key regulatory agencies, as well as industry best practices.

▣ Why HIPAA is Insufficient to Meet the Challenges Posed by E-Health

The HIPAA Privacy Rule was a landmark in privacy protection, but it is widely recognized that the regulation is insufficient to adequately cover the new and rapidly evolving e-health environment. For example:

- The HIPAA Privacy Rule covers only certain "covered entities" as defined in the HIPAA statute: specifically, providers, plans, and healthcare clearinghouses. Many of the new entities storing, handling or managing personal health information electronically do not qualify as covered entities, and thus are not directly covered by the Privacy Rule. In some cases, other federal privacy laws may apply, but only in specific and limited contexts. As a result, we do not have a baseline set of federal health privacy protections that apply to all entities that handle personal health information. For example, state and regional health information organizations or health information exchanges (also known as RHIOs or HIEs), which may aggregate and/or facilitate exchange of personal health information, may not be covered by the Privacy Rule.⁸ Further, sensitive health data in

⁸ In December 2008 HHS issued guidance clarifying that health information networks that merely exchange data on behalf of covered entities must be business associates, but such guidance does not cover all of the network models currently in existence or in development.

personal health records offered by employers and Internet companies also is not protected by federal health privacy law.

- The Privacy Rule is based on a model of one-to-one electronic transmission of health information among traditional health care system entities and their business partners who perform health-related functions on their behalf. The Rule does not adequately account for new health information networks, which allow broader access to greater volumes of identifiable health information.
- Personal health data is migrating onto the Internet through an exploding array of health information sites, online support groups, and other on-line health tools, not covered by HIPAA but regulated only through enforcement by the Federal Trade Commission (FTC) of the general prohibition against unfair and deceptive trade practices, such as a failure to follow promised privacy policies.
- HIPAA has never required that patients receive notice when their personal health information is inappropriately accessed or disclosed.
- The HIPAA Privacy Rule does not make it clear that patients are entitled to an electronic copy of their records, so patients themselves can transfer their records to other digital services if desired.
- The Privacy Rule's requirements with respect to "marketing" are weak and far too often permit entities to use patients' protected health information without their prior authorization to send them marketing materials regarding health care products or services. The deficiencies in the current rule may be exacerbated by the need of these nascent health data exchanges to find a viable business model to sustain start-up and long-term expenses – a need that these exchanges may seek to fulfill with advertising and other commercial re-uses of patient data.
- The HIPAA rules currently provide no incentive for covered entities to de-identify data or strip it of common patient identifiers before it is used for routine functions such as those contained in the definition of "health care operations," even though, in many instances, these legitimate purposes could be accomplished without using personally identifiable information.

▣ Ensuring Accountability for All Entities Engaged in e-Health

As noted above, the HIPAA Privacy and Security Rules set forth requirements for the handling of individually identifiable health information by covered entities and their business associates (entities that contract with covered entities to perform functions on their behalf). Not all entities handling personal health

information are covered by the rules. In addition, the HIPAA rules were intended to set only a basic floor of protections. To establish an environment of trust that will facilitate the widespread implementation of health IT, all entities handling health information should develop and implement health information policies beyond what HIPAA may require.

The economic recovery legislation will devote an unprecedented level of taxpayer resources to the development and implementation of health IT to improve health care and lay the foundation for further health reform efforts. Persons and entities receiving such federal funds should be held accountable, both for how they use the funds, as well as for adopting and implementing the policies and technological solutions necessary to protect medical data they store and share.

The stimulus legislation includes provisions to strengthen HIPAA, and to establish a process for developing baseline privacy protections that will apply to personal health information held by entities not covered by HIPAA. However, the bill should go further to ensure that health IT is governed by a comprehensive framework of protections that builds public trust and enables the sharing of information for core health care functions. Therefore, Congress should consider adding to the bill language explicitly directing the HHS Secretary to establish policies and programs to ensure: that all entities who receive federal funds for health IT are held accountable for their use of the funds; that they adopt and implement policies and technological solutions addressing each of the core privacy principles identified in this testimony; and that they are held accountable for complying with such policies and other applicable law. Such language would help assure that, regardless of whether HIPAA applies or adequately covers an entity, there is a comprehensive framework of policies in place to protect health information and sufficient oversight and accountability for compliance with that framework. The Secretary should also be required to regularly report to Congress on how funds have been spent and how such privacy and security policies have been implemented.

■ Strengthening HIPAA Privacy and Security Rules to Meet New Challenges

With respect to the access, use and disclosure of electronic health information by the traditional players in the health care system, there are some immediate steps Congress should take to fill gaps in HIPAA. The economic recovery legislation under consideration by Congress takes concrete steps toward filling these gaps and establishing the comprehensive framework of protections that will build public trust in health IT. For example:

Right to Be Notified in the Event of a Breach

The proposed legislation establishes a federal right to be notified in the event of a breach of protected health information, and such breach notification provisions apply to HIPAA-covered entities and their business associates as well as to any other commercial entities that maintain personal health information. These provisions would establish for the first time a national right for consumers to at least be notified when the security of their health information is compromised; currently, only three state breach notification laws expressly apply to health data.⁹ Further, the proposed legislation does not require notification when the information that is breached has been rendered inaccessible to unauthorized persons via encryption or a similar technology. This provides a powerful incentive for entities holding personal health information to adopt strong encryption-type controls, significantly minimizing the likelihood of data breach.

Some industry stakeholders are calling for a “harm” standard for breach notification —i.e., patients need only be notified if there is the potential for financial loss or tangible harm, such as loss of a job or insurance. Such standards may be appropriate for breaches of financial data, where harm can be more easily quantified and remedied, but health information is not the same as financial information. Once sensitive medical data is in the public domain or in the hands of an unauthorized person, it cannot be taken back, and the potential harm is difficult to quantify and often subjective (what is sensitive to one person may not be sensitive to another). If harm were the trigger for notification, entities breaching the data would have too much discretion to decide whether the risk of harm to the patient is worth the burden (and potential damage to institutional reputation) of notifying. The provisions in the legislation take the subjectivity out of the decision – and provide strong incentives for entities holding medical data to protect it with encryption-type technologies.

Strengthening Prohibitions Against Unauthorized Use of Data for Marketing Purposes

As noted above in our testimony, more than three-fourths of consumers are concerned about the use of their health information for marketing purposes. The benefits of health IT will not be realized if entities that have access to personal health information are allowed to use it without individual authorization for marketing purposes.

⁹ Arkansas, California and Delaware. Deborah Gage, California data-breach law now covers medical information, *SF Gate* (January 4, 2008), See <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/01/04/BUR6U9000.DTL>.

Although HIPAA already prohibits use of health information for marketing without patient authorization, the HIPAA definition of marketing includes significant exceptions.¹⁰ These exceptions permit the use of a patient's personal information without consent to facilitate communications from health care providers and plans that can be characterized as patient education— for example, information on treatment alternatives, or benefit options, or care management tools. In fact, the only health-related communications that are clearly marketing – and prohibited without express patient authorization – are those made directly to a patient by a third party selling a product or service, where the covered entity has provided the third party with the personal information that facilitates the making of the communication.¹¹ However, if the same communication is sent by the covered entity to the patient, it is not marketing – even if the covered entity is paid by the third party to make the communication on its behalf.

The proposed legislation deals with this issue in three ways: (1) by prohibiting the sale of “protected” (identifiable) health information, (2) by making it clear that communications sent by covered entities that are paid for by outside entities are marketing and therefore require prior authorization from the patient, and (3) by requiring covered entities to obtain prior patient authorization before sending fundraising solicitations.

Some claim that these provisions will prohibit the sending of important health communications like flu shot and drug refill reminders. Current HIPAA rules allow covered entities, including providers, health plans and pharmacies, to use patient identifiable information to send these communications without patient authorization, and the provisions in the stimulus legislation do nothing to alter those rules. Instead, they target the inappropriate influence from outside entities over the types of communications sent to patients without their prior authorization. They also make it clear patient information cannot be used for fundraising purposes without a patient's prior authorization. Finally, by including a strong prohibition against the sale of medical records and identifiable personal health information, the legislation attacks current practices that violate patient trust and helps ensure that advances in health information exchange are not inappropriately exploited for commercial gain. These improvements in the rules regarding use of personal health information for marketing and other commercial purposes would greatly enhance patient trust in e-health systems.

¹⁰ 45 C.F.R. §164.501.

¹¹ Office of Civil Rights Brief, Summary of the HIPAA Privacy Rule, p. 9-10.

Giving Patients a Meaningful Right to Monitor Disclosures from Their Medical Records

The HIPAA Privacy Rule gives patients the right to receive an “accounting” of certain disclosures of their health information – but this right does not apply to routine disclosures for treatment, payment or health care operations. Electronic technologies can provide covered entities the ability to track precisely who has accessed a patient’s medical record. CDT understands that a number of entities using electronic health records are already employing these electronic “audit trails” to control who can access a patient’s record and to internally monitor who is accessing patient records and for what purposes.

The proposed legislation would phase in a requirement for all entities using electronic health records to track disclosures from the record and allow patients, upon request, to receive a copy of such disclosures over a three-year period. When this provision was included in legislation considered in the House of Representatives in the 110th Congress, health care providers and plans weighed in with a number of concerns. Fortunately, these concerns have been addressed in the proposed legislation. For example, the provision directs the Secretary to issue regulations about what must be included in the accounting, taking into account administrative burdens and the needs of patients. Further, the requirement does not go into effect until these regulations are promulgated and standards are adopted that will ensure medical records have the technology in place that will allow them to comply. Entities with existing systems that may not have the technical capacity to comply have until 2014 to come into compliance; those who adopt newer systems must comply by 2011.

Examination of “Health Care Operations”

Under the current Privacy Rule, patient consent is not required for covered entities to use personal health information for health care operations. The definitions of treatment and payment are relatively narrow; however, health care operations encompasses a much wider range of activities, including administrative, financial, legal, and quality improvement activities (see footnote for a complete list).¹² Privacy and consumer advocates have long been

¹² Health care operations include: (1) Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination; (2) Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities; (3) Underwriting and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to health care claims; (4) Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs; (5) Business Planning and development, such as conducting cost-management and planning analyses related to managing and operating the entity; and (6) Business management and general administrative

concerned that health care operations permits the use of personal health information for a broader range of purposes than should be permitted under fair information practices.

The proposed legislation addresses this issue by requiring the HHS Secretary to re-examine the health care operations definition and consider whether some functions within this definition should require prior patient authorization. The Secretary is also tasked to consider whether some operations functions can and should be done with de-identified health data (for example, activities such as quality improvement, peer review and credentialing, and business planning). De-identified data has been stripped of a number of common patient identifiers, and thus its use for routine business purposes poses less privacy risk (as long as it is protected from re-identification). We hope HHS will also look at crafting more narrow definitions of, or providing more detailed guidance regarding, some of the broad terms used in health care operations (such as “case management and care coordination”) to ensure they are defined to include only core health care functions. Further, as explained in more detail below, the Secretary should also consider using the current “minimum necessary” standard to encourage or require the use of anonymized data to perform many routine health care operations functions.

Clarification of Minimum Necessary

A critical element of fair information practices is that data collection should be limited to what is needed to meet the particular purpose for which the data is lawfully sought. The HIPAA Privacy Rule requires covered entities to request – and use and disclose – only the *minimum amount* of information necessary to accomplish their legitimate purposes, except when information is being used or disclosed for treatment purposes. The minimum necessary provisions are broadly worded and meant to be flexible to respond to the particular context. Unfortunately, covered entities often say that they are confused by the minimum necessary rule – and the frequent result is misinterpretation of the law.

The proposed legislation takes concrete steps toward clarifying this provision. Most importantly, the legislation requires the Secretary to issue guidance on what constitutes “minimum necessary.” As the Secretary is developing this guidance, covered entities are directed to use a “limited data set,” which is data stripped of a number of common patient identifiers, to meet the minimum necessary requirements. However, in circumstances where the limited data set

activities, including those related implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity. 45 C.F.R. §164.501.

would be insufficient to meet the covered entity's legitimate purposes for accessing or disclosing the data, entities may use the amount of identifiable data necessary to fulfill that purpose.

In developing guidance on minimum necessary, the Secretary should consider whether fully identifiable patient data is needed to accomplish all the activities currently included in health care operations, and whether data scrubbed of common patient identifiers, which provides greater privacy protection for patients, could serve covered entities' needs to access data without being unduly burdensome. (Such a review should be part of the Secretary's examination of health care operations, which is included in another provision of the legislation and discussed above.) For example, today covered entities may use fully identifiable data for quality assessment and improvement activities, peer review of health professionals, accreditation or credentialing, performing audits, and business planning. For each of these activities, covered entities need access to data about the care that was provided, but in most cases they do not need information that is identified to a particular patient. Using data that has been stripped of key patient identifiers can help protect privacy while allowing the use of data for important health-related functions.

The Privacy Rule includes provisions for two types of anonymized data – the limited data set and de-identified data. However, these data sets require the masking of too much data to be useful for some operations purposes. In issuing guidance on minimum necessary, HHS should set forth additional options for use of data stripped of common patient identifiers for health care operations.

Ensuring Electronic Access for Patients

The HIPAA Privacy Rule provides individuals with a right to access and receive a copy of their medical records, "in the form or format requested," if those records are "readily producible" in that format.¹³ However, the access right in the HIPAA rule has not been well implemented. The failure to disclose to patients their medical records - even in paper format - is one of the top five HIPAA complaints investigated by HHS.¹⁴ In addition, the Privacy Rule allows covered entities to charge a "reasonable cost" for copying a patient's record, which reportedly range from free to \$37.00 for up to 10 pages.¹⁵ The proposed

¹³ 45 C.F.R. 164.524(a) & (c) (such access right is for information maintained in a designated record set).

¹⁴ HHS, Compliance and Enforcement, Top Five Issues in Investigated Cases Closed with Corrective Action, by Calendar Year, <http://www.hhs.gov/ocr/privacy/enforcement/data/top5issues.html>.

¹⁵ State laws may set limits on copying charges for records, which range from free for the first copy (Kentucky) to \$37.00 for up to the first 10 pages of a hospital-based record (Texas). See <http://hpi.georgetown.edu/privacy/records.html> for more information.

legislation addresses this by making it clear that patients have the right to an electronic copy of their medical records at a nominal cost when those records are kept electronically. Congress should strengthen this provision by adding language to clarify that this right of electronic access extends to having an electronic copy sent directly to the individual's electronic personal health record.

■ Establishing Privacy Protections for Personal Health Records

Personal health records (PHRs) and other similar consumer access services and tools now being created by Internet companies such as Google and Microsoft, as well as by employers, will not be covered by the HIPAA regulations unless they are being offered to consumers by covered entities. In this unregulated arena, consumer privacy will be protected only by the PHR provider's privacy and security policies (and potentially under certain state laws that apply to uses and disclosures of certain types of health information), and if these policies are violated, the Federal Trade Commission (FTC) may bring an action against a company for failure to abide by its privacy policies. The policies of PHR vendors range from very good to seriously deficient.¹⁶ The absence of any clear limits on how these entities can access, use and disclose information is alarming – and has motivated some to suggest extending the HIPAA Privacy Rule to cover PHRs. But we believe that the Privacy Rule, which was designed to set the parameters for use of information by traditional health care entities, would not provide adequate protection for PHRs and may do more harm than good in its current scope. Further, it may not be appropriate for HHS, which has no experience regulating entities outside of the health care arena, to take the lead in enforcing consumer rights and protections with respect to PHRs.

The proposed legislation – which tasks HHS and FTC with jointly coming up with recommendations for privacy and security requirements, as well as breach notification provisions, for PHRs – proposes the right approach for ultimately establishing comprehensive privacy and security protections for consumers using these new health tools. For PHRs offered by entities that are not part of the traditional health care system, it is critical that regulators understand the business model behind these products, which will largely rely on advertising revenue and partnerships with third-party suppliers of health-related products

¹⁶ The HHS Office of the National Coordinator commissioned a study in early 2007 of the policies of over 30 PHR vendors and found that none covered all of the typical criteria found in privacy policy. For example, only two policies described what would happen to the data if the vendor were sold or went out of business, and only one had a policy with respect to accounts closed down by the consumer.

and services. Relying solely on consumer authorization for use of information shifts the burden of protecting privacy solely to the consumer and puts the bulk of the bargaining power on the side of the entity offering the PHR. For consumers to truly trust PHRs – and for these tools to flourish as effective mechanisms for engaging more consumers in their health care – clear rules are needed regarding marketing and commercial uses that will better protect consumers. The legislation lays the foundation for the establishment of these rules, and tasks the FTC with enforcing breach notification provisions until these rules can be established.

In establishing protections for information in PHRs, policymakers need not start from scratch. The Markle Foundation's Connecting for Health initiative last year released a "Common Framework for Networked Personal Health Information" that sets forth practices to protect personal information and enhance individual participation in online personal health records.¹⁷ This framework, developed through a multi-stakeholder, public-private collaboration and endorsed by major PHR vendors and leading consumer groups, could guide both governmental policies and industry best practices.

Strengthening HIPAA Enforcement

When Congress enacted HIPAA in 1996, it included civil and criminal penalties for failure to comply with the statute, and these penalties applied to the subsequent privacy and security rules implemented years later. Unfortunately, the HIPAA rules have never been adequately enforced. As noted above, HHS has not levied a single penalty against a HIPAA-covered entity since the rules were implemented.¹⁸ The Justice Department has levied some penalties under the criminal provisions of the statute – but a 2005 opinion from DOJ's Office of Legal Counsel (OLC) expressly limits the application of the criminal provisions to covered entities, and prosecutors seeking to enforce criminal penalties against individuals have had to rely on other federal laws.¹⁹

¹⁷ See www.connectingforhealth.org/phti for further information.

¹⁸ In July 2008, HHS announced that Seattle-based Providence Health & Services agreed to pay \$100,000 as part of a settlement of multiple violations of the HIPAA regulations. But the press release from HHS made clear that this amount was not a civil monetary penalty. <http://www.hhs.gov/news/press/2008pres/07/20080717a.html>.

¹⁹ See <http://www.americanprogress.org/issues/2005/06/b743281.html> for more information on the OLC memo and the consequences; see also P. Winn, "Who is Subject to Criminal Prosecution under HIPAA," 2005, http://www.abanet.org/health/01_interest_groups/01_media/WinnABA_2005-11.pdf.

In addition, business associates who access, use and disclose protected health information on behalf of covered entities are accountable for complying with HIPAA privacy and security regulations only through their contracts with covered entities. If the covered entity does not take action to enforce the contract, there is no other mechanism for ensuring that the business associate complies with the applicable rules. Further, HHS can only hold the covered entity responsible for the actions of business associates only if the entity knew of a "pattern of activity or practice of the business associate that constituted a material breach or violation" of its agreement with the covered entity, and the covered entity doesn't take action to cure the breach or terminate the contract.²⁰ Of interest, if the covered entity decides that terminating the contract is "not feasible," the covered entity is required to report the problem to the Secretary.²¹ But the regulations do not give the Secretary any further authority to enforce HIPAA against the business associate or hold the covered entity responsible for the violation.

A lax enforcement environment sends a message to entities that access, use and disclose protected health information that they need not devote significant resources to compliance with the rules. Without strong enforcement, even the strongest privacy and security protections are but an empty promise for consumers. Further, even under the existing enforcement regime, there is no ability for consumers whose information is accessed or disclosed in violation of HIPAA to seek redress or be made whole.

The proposed legislation includes a number of provisions strengthening enforcement of HIPAA and providing a mechanism for individuals whose privacy has been violated to receive some compensation:

Accountability for Business Associates

The proposed legislation closes this loophole by ensuring that business associates can be held legally accountable for complying with the HIPAA Security Rule and with those provisions of the Privacy Rule that apply to their contractual activities. The legislation does not impose additional obligations on business associates with respect to complying with the Privacy Rule (beyond the additional requirements imposed by the legislation on both covered entities and business associates); instead it ensures accountability to federal authorities when there is a failure to comply.

²⁰ 45 C.F.R. 164.504(e)(ii).

²¹ *Id.*

Strengthened Statutory Provisions Authorizing Criminal and Civil Penalties

To remedy the effect of the Bush OLC memo, the proposed legislation makes it clear that criminal penalties can be assessed against individuals for intentional violations of HIPAA. To ensure that the most egregious HIPAA violations do not go unpunished, the legislation also clarifies that the Secretary can bring an action for civil monetary penalties in circumstances where a criminal violation of HIPAA may have occurred but the Justice Department decides not to pursue the case.

The HIPAA statute requires that the Secretary impose civil monetary penalties for HIPAA violations.²² Another part of the statute provides the Secretary with the authority to give covered entities the chance to correct the violation, or to adjust the amount of the penalty, but only in cases where the entity did not know (and reasonably could not have known) of the violation or the violation was due to reasonable cause.²³ Unfortunately, under the Bush Administration, HHS issued regulations requiring the Secretary to first try to informally resolve *all* HIPAA complaints, and the agency pursued a policy of voluntary compliance and handled most complaints informally, even in cases where the violation rose to the level of willful neglect. The proposed legislation ensures that civil monetary penalties will be imposed in the most egregious civil cases – those involving willful neglect of the law – by requiring the Secretary to investigate all complaints for which a preliminary inquiry into the facts indicates possible willful neglect and pursue civil monetary penalties in willful neglect cases. The legislation still permits the Secretary to allow for corrective action, and to informally resolve, those cases involving reasonable cause, and where the entity did not know, and reasonably could not have known, of the violation.

Finally, the proposed legislation increases the civil monetary penalties for HIPAA violations, and creates a tiered penalty structure, so that more serious violations are penalized at a higher level. Except in cases of willful neglect, the Secretary may not impose a penalty if the offense is corrected within a 30-day time period and may adjust the amount of the penalty to match the severity of the offense.

Enhancing Enforcement Resources

The proposed legislation also requires that any penalties or settlements collected be directed to HHS for use in enforcing the Privacy and Security Rules and

²² See Section 1176(a) of the Social Security Act (“...The Secretary *shall* impose on any person who violates a provision of this part a penalty of not more than \$100 for each such violation, except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a calendar year may not exceed \$25,000).

²³ Section 1176(b)(2) & (3) of the Social Security Act.

expressly authorizes State Attorneys General to enforce HIPAA. The HHS Office of Civil Rights is significantly under resourced, and devoting greater resources – in both dollars and manpower - should help ensure greater accountability for compliance with HIPAA. Currently, only those State Attorneys General who expressly have the authority to enforce federal law by state statute are able to enforce the federal HIPAA provisions. State authorities are able to enforce their own state health privacy laws, but in only a handful of states are those laws as comprehensive as HIPAA. The provisions in the proposed legislation ensure that entities subject to HIPAA will not be prosecuted simultaneously by state and federal authorities.

Providing Consumers with Meaningful Recourse

A significant shortfall in HIPAA is the absence of any way for the consumer whose health information privacy has been violated to pursue meaningful recourse and be made whole. As noted above, the HIPAA statute already provides for criminal and civil monetary penalties, but these penalties do not currently go to the consumers whose privacy was violated. The proposed legislation directs GAO to recommend methodologies for individuals to receive a percentage of any penalties or monetary settlements collected for violations of HIPAA, and within three years the Secretary is required to establish such a methodology by regulation.

Strengthened Accountability to Congress, Raised Visibility of Importance of Privacy

Finally, the proposed legislation requires HHS to annually report to Congress on enforcement of the HIPAA rules and establishes privacy officers in each HHS regional office, which support better enforcement by both increasing Congressional scrutiny and raising the visibility of privacy as an HHS priority. As noted above, Congress should consider strengthening the legislation to ensure accountability for establishing and complying with privacy and security policies that go beyond HIPAA requirements, or for entities not covered by HIPAA.

■ Other Notable Provisions in the Stimulus Bill

- While the Privacy Rule includes criteria for de-identifying data, these criteria are now more than five years old – and new technologies and the increased availability of data on-line make it much easier to re-identify once de-identified health information. The proposed legislation tasks HHS with coming up with guidance on how best to implement the HIPAA Privacy Rule requirements on deidentification, providing an opportunity for an update to these provisions. CDT hosted a day-long workshop on de-

identification of data last fall, and a paper summarizing the proceedings of that workshop and suggesting areas of further inquiry is in progress.

- The proposed legislation authorizes \$10 million for a comprehensive national education initiative to enhance public transparency regarding uses of health information and the effects of such uses.
- The legislation also makes it clear that stronger state privacy rules are preserved, which has always been an important component of HIPAA.

▣ The Appropriate Role of Consumer Consent

Recently, public debates about how best to protect the confidentiality, privacy and security of health information have focused almost exclusively on whether patients should be asked to authorize all uses of their health information. The ability of individuals to have some control over their personal health information is important, and a comprehensive privacy and security framework should address patient consent.²⁴ HIPAA requires prior patient authorization before certain types of information can be accessed or disclosed, or when information is being sought for purposes like marketing or, in most circumstances, research. The proposed legislation attempts to strengthen the role of consent by requiring covered entities to honor a patient's request to restrict disclosure for payment and health care operations purposes when the patient has paid out-of-pocket for all costs of care. It is critical that where consent is either required or voluntarily sought, health information systems are structured in a way that allows these consents to be honored and appropriately and securely managed.

But patient authorization is not a panacea, and as appealing as it may appear to be in concept, in practice reliance on consent would provide weak protection for consumer's health information. If health privacy rules fail to address the range of privacy and security issues through concrete policies, and instead rely only (or significantly) on giving individuals the right to consent to multiple uses and disclosures of their personal health information, the result is likely to be a system that is *less* protective of privacy and confidentiality.

Just yesterday CDT released a paper calling for a rethinking of the appropriate role of consent in health care, which sets forth in more detail why consent is not the sine qua non of privacy protection. (www.cdt.org/healthprivacy) Among other reasons, a consent-based system places most of the burden for privacy

²⁴ In addition, much more should be done to improve the way in which consent options are presented to consumers in the healthcare context. Internet technology can help in this regard, making it easier to present short notices, layered notices and more granular forms of consent.

protection on patients at a time where they may be least able to make complicated decisions about use of their health data. If consent becomes the focus of privacy protection, it is clear that patients will be exposed to unregulated and potentially unanticipated uses—and misuses—of their data. Further, if policymakers rely on consent by an individual for any particular use of his or her information as the key to privacy protection, the healthcare industry will have fewer incentives to design systems with stronger privacy and security protections.

In contrast, a comprehensive approach – which allows health information to flow for core purposes with consent but also establishes clear rules about who can access, use and disclose a patient’s personal health information and for what purposes – puts the principal burden on the entities holding this information. The proposed legislation takes concrete steps toward this comprehensive approach.

■ Conclusion

To establish greater public trust in HIT and health information exchange systems, and thereby facilitate adoption of these new technologies, a comprehensive privacy and security framework must be in place. From traditional health entities to new developers of consumer-oriented health IT products to policymakers, all have an important role to play in ensuring a comprehensive privacy and security framework for the e-health environment. In the economic recovery legislation, Congress must set the framework for privacy and security by: ensuring that all holders of personal health information adopt and are held accountable for complying with a comprehensive privacy framework; filling the gaps in HIPAA’s protections; enacting new standards for commercial entities who hold and exchange health information; and strengthening enforcement of existing law.

Thank you for the opportunity to present this testimony in support of the need for a trusted health information sharing environment to support health IT and the provisions in the proposed economic stimulus legislation. These provisions move the nation much closer to securing comprehensive, workable privacy and security protections for electronic health information systems. I would be pleased to answer any questions you may have.

CENTER FOR
DEMOCRACY
TECHNOLOGY

FOR MORE INFORMATION

Please contact: Deven McGraw, (202) 637-9800 x 119, deven@cdt.org

STATEMENT OF
DAVID MERRITT
PROJECT DIRECTOR,
CENTER FOR HEALTH TRANSFORMATION*
BEFORE THE SENATE JUDICIARY COMMITTEE
TUESDAY, JANUARY 27, 2009

Chairman Leahy, Senator Specter, and members of the committee:

Thank you for the opportunity to testify about how to modernize our healthcare system through information technology while protecting patient privacy.

Information about our health and healthcare is by far the most sensitive data a person owns. From chronic conditions to medications to genetic makeup, our personal health information reveals intimate details about who we are, what we do, and what we may be like in the future. Thus, protecting our privacy and confidentiality is a principle that simply cannot be compromised.

However, as the pace quickens to modernize healthcare through information technology, such as through the adoption of electronic health records, there is a growing tension between protecting personal data and having instant access to it when it is needed.

On the one hand, having real-time access to personal health information can often mean the difference between life and death. On the other hand, the loss of such sensitive data to outsiders, especially those with nefarious or self-interested intentions, can have disastrous and long-term consequences.

The Congress has started an important conversation of how policy can help balance progress and privacy: Progress toward building an electronic health system and protecting the privacy of those who are part it.

This must be done exactly right. For if there are onerous restrictions or cumbersome administrative burdens on physicians, health systems, and other providers, then they will not adopt new technology, and patients will suffer by not

* The Center for Health Transformation, founded and led by former Speaker of the House Newt Gingrich, is a collaboration of leaders dedicated to the creation of a 21st Century Intelligent Health System that saves lives and saves money for all Americans. For more information on the Center and our Health Information Technology project, please visit www.healthtransformation.net.

receiving the best possible care. If restrictions on electronic data exchange are too excessive, new breakthroughs that can be found by researching de-identified patient data will not happen. The widespread adoption of information technologies and the use of new research tools are desperately needed to bring our healthcare system out of the Stone Age. Delivering better care at lower cost cannot happen without them.

However, if these IT systems lack adequate privacy protections, whether real or perceived, then consumers will likely shy away from providers who have adopted new technology and perhaps not get the care they need or the better quality care that can be delivered with IT.

We need to find the right balance between privacy at all costs and progress at any cost.

Other industries

One approach is to look outside of healthcare. Healthcare is not the first industry to undergo a shift from paper to modern, electronic tools. (In fact, it is the last.) We can learn how other industries have balanced progress with privacy, from financial services and online banking to online shopping and ATMs. How did these technologies prosper and grow while protecting privacy and security? Certainly there are continuing issues to address, but healthcare can learn from their experiences and adopt what works.

Going back decades, innovators and entrepreneurs have long sought how to protect and secure data while making it portable. In 1984, D.W. Davies and W.L. Price published *Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer*. The publisher noted that the book addressed, "How to use cryptography to protect data in teleprocessing systems--not only keeping data secret but also authenticating it, preventing alteration, and proving its origin."

Today virtually every bank in the United States offers online banking, where we can transfer money from one account to another; pay bills; view statements; and securely communicate with bank representatives. Financial data is not quite as sensitive as personal health information, but it is close. And consumers must still make the decision on whether to use information technology to share, post, and/or store their data online—or to be customers of institutions that do this.

Security and privacy are common concerns among consumers, and there are privacy and security vulnerabilities to address. A recent study found that security flaws in online banking services were widespread, endangering personal financial information.¹ Despite this, Americans increasingly trust and use the technology.

¹ Atul Prakash, University of Michigan, Department of Electrical Engineering and Computer Science, "Analyzing Web sites for user-visible security design flaws." July 2008. <http://www.ns.umich.edu/htdocs/releases/story.php?id=6652> (Accessed January 23, 2000).

The Pew Internet & American Life Project reported this month that 55 percent of Americans have used online banking services.²

The same can said for e-commerce or online retailing. Credit card fraud, identity theft, and phishing are real threats for consumers that can compromise bank accounts, passwords, and other sensitive data. *The Washington Post* reported last summer that a Russian cyber-crime gang had compromised more than 378,000 computer systems over a sixteen-month period.³

Despite the threats e-commerce continues to grow at a remarkable pace. The Census Bureau reported that total e-commerce sales in 2007 were \$136 billion, a 19 percent increase from 2006.⁴ Online sales now account for 3.4 percent of all retail sales in the U.S., a nearly six-fold increase since 1999.⁵

Consumers know the risks, but they have increasing faith that online services are secure and their financial data is safe. And these services are, for the most part, incredibly secure. Technology programmers from across the globe have worked tirelessly to build secure hardware, software, and networks that protect privacy and sensitive data.

One of the key reasons for success has been technical cooperation throughout the industry to develop common, uniform standards of data transmission. From electronic signatures and security certificates to authentication rules and data encryption, common standards allow for the safe, secure sharing of information that protects privacy. Organizations like the American National Standards Institute (ANSI), International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Federal Financial Institutions Examination Council, and the Payment Card Industry Security Standards Council have collaborated to create a common foundation to securely share sensitive information.

The healthcare industry is working with many of these organizations, as well as others, to create common data standards of securely sharing personal health information while protecting privacy.

What is healthcare doing?

Much of the industry collaboration has been done through organizations like Integrating the Healthcare Enterprise (IHE), Health Level Seven (HL7), the

² Pew Internet & American Life Project, Latest Trends, January 2009.

http://www.pewinternet.org/trends/Internet_Activities_Jan_07_2009.htm (Accessed January 23, 2009).

³ Brian Krebs, "Online Crime Gang Stole Millions," *Washingtonpost.com*, August 7, 2008.

http://voices.washingtonpost.com/securityfix/2008/08/online_crime_gang_stole_millio.html (Accessed January 23, 2009).

⁴ U.S. Census Bureau, Quarterly Retail E-commerce Sales 4th Quarter 2007, Released February 15, 2008.

<http://www.census.gov/mrts/www/data/html/07Q4.html> (Accessed January 23, 2009).

⁵ *Ibid.*

CORE initiative of the Council for Affordable Healthcare Quality (CAQH)*, the Healthcare Information Technology Standards Panel (HITSP), and the Certification Commission for Healthcare Information Technology (CCHIT).** The latter two are of particular importance.

HITSP is a cooperative partnership between the public and private sectors, operated under the aegis of ANSI. Its mission is to “harmonize and integrate standards that will meet clinical and business needs for sharing information among organizations and systems.”⁶ Created through the leadership of former HHS Secretary Mike Leavitt and former National Coordinator for Health Information Technology David Brailer, one of its key priorities has been to develop industry standards on securely sharing personal health information while protecting patient privacy.

Much progress has been made. Through the Security, Privacy & Infrastructure Domain Technical Committee, HITSP has finalized and released a series of industry-wide technical standards that can be incorporated into IT products to secure personal health information and control access to it.

The following selected standards and specifications have been recognized or released—ranging from patient consent directives and access controls to data anonymization and audit trails—and all can secure sensitive information and give patients control over their data.

TP 20 - Access Control Transaction Package

The Access Control Transaction Package provides the mechanism for security authorizations which control the enforcement of security policies including: role-based access control; entity based access control; context based access control; and the execution of consent directives. An example of this is a functional role that has the permission to perform an act (e.g., consumer updating a Personal Health Record (PHR)). In an emergency, this construct must support the capability to alter access privileges to the appropriate level (failsafe/emergency access), which may include override of non-emergency consents.

TP 30 - Manage Consent Directives Transaction Package

The Manage Consent Directives Transaction Package describes the messages needed to capture, manage, and communicate rights granted or withheld by a consumer to one or more identified entities in a defined role to access, collect, use or disclose individually identifiable health information (IIHI), and also supports the delegation of the patient's right to consent. The transactions described in this construct are intended to be carried out by HITSP/TP13 - Manage Sharing of Documents.

T 15 - Collect and Communicate Security Audit Trail Transaction

The Collect and Communicate Security Audit Trail Transaction is a means to provide assurance that security policies are being followed or enforced and that risks are being mitigated. This document describes the mechanisms to define and identify security relevant events and the data to be collected and communicated as determined by policy, regulation or risk analysis. It also provides the mechanism to determine the record format to support analytical reports that are needed.

T 17 - Secured Communication Channel Transaction

The Secured Communication Channel Transaction provides the mechanisms to ensure the

* CAQH is a member of the Center for Health Transformation.

** Disclosure: I am a member of the Board of Commissioners for CCHIT. However, the views expressed here are mine and do not necessarily represent those of CCHIT.

⁶ Health Information Technology Standards Panel, www.hitsp.org. (Accessed January 23, 2009.)

authenticity, integrity, and confidentiality of transmissions, and the mutual trust between communicating parties. Its objectives include providing: mutual node authentication to assure each node of the others' identity; transmission integrity to guard against improper information modification or destruction while in transit; and transmission confidentiality to ensure that information in transit is not disclosed to unauthorized individuals, entities, or processes.

C 19 - Entity Identity Assertion Component

The Entity Identity Assertion Component provides the mechanisms to ensure that an entity is the person or application that claims the identity provided. An example of this Component is the validation and assertion of a consumer logging on to a Personal Health Record (PHR) system.

C 25 - Anonymize Component

The Anonymize Component provides specific instruction for anonymizing data that are prepared for repurposing data created as part of routine clinical care delivery. This construct defines the Component specification that provides the ability to anonymize patient identifiable information.

Source: Health Information Technology Standards Panel

This is real progress on actually delivering security and patient control to ensure privacy. Now that these standards are available, it is up to information technology vendors to implement them in their products. One way to drive this is through the certification process of CCHIT.

The mission of CCHIT is "to accelerate the adoption of robust, interoperable health information technology by creating a credible, efficient certification process." It tests a range of products, including electronic health records, to ensure that products meet a certain level of functionality, interoperability, and security.

According to CCHIT, in its document entitled "CCHIT Certification – What Does It Require?," the certification process requires ambulatory EHR products to provide state-of-the-art technical capabilities needed to keep patient information safe and secure. There are approximately 50 security criteria. To be certified, an EHR must meet 100 percent of these criteria. The broad areas covered include:

- Authentication of users (proving identity);
- Controlling access based on the user role or the context of a care situation;
- Auditing every access and use of a record;
- Encryption of any data sent out of a system;
- Protection against viruses and other malware; and
- Backup of data to prevent loss in case of computer failure or disaster.

Standards identified by HITSP are transferred to CCHIT, where the implementation of those standards in actual products is verified. Every certified electronic health record product must meet these requirements. The information that is captured and stored using certified products is secure, which in turn goes a long way to protecting patient privacy. As HITSP continues to develop and improve security and privacy data standards, they will become additional criteria for certification and, in turn, integrated into the marketplace.

On a general note, policymakers are currently debating the future of HITSP and CCHIT, as well as the National eHealth Collaborative (NeHC), formerly known as

the American Health Information Community. One question under consideration is whether these organizations should continue their work or be replaced or diminished by new organizations. I cannot state in stronger terms that these organizations should continue and that no new organizations should be created.

Some have argued that they have not delivered widespread adoption of health information technology. Several years ago two of the biggest cries were that no entity existed to certify products with a "seal of approval" and that there was no industry-wide movement to develop common data standards. By addressing those concerns, HITSP and CCHIT have indeed contributed to adoption. The single most important missing piece to expedite adoption is realigning provider incentives. Healthcare payers, both public and private, must collaborate with providers to overcome the well-documented financial barriers to adoption.

Others argue that these organizations be replaced because they have not created a finalized, perfected framework of interoperability standards. This is certainly true, in that comprehensive interoperability is not yet a reality, but these organizations have laid far more groundwork in their three to four years of operation than was accomplished in the previous twenty.

Still others argue that the federal government should be a more active leader in driving these processes. One of the key advantages of the current governance is that it truly is a public-private partnership. The federal government is represented and actively participates in HITSP, CCHIT, and NeHC. This balance is necessary. It combines the expertise and market presence of private industry with the purchasing and regulatory power of government.

Replacing these organizations now with new organizations or confusing the marketplace with parallel organizations, requirements, and processes literally turns the clock back four or five years, when the industry first debated this kind of governance. If the existing governance is not given time to work, if we revisit this debate now, the entire industry will pay a huge opportunity cost in time and resources.

To be sure, there are improvements that can be made. HITSP should have firm, aggressive deadlines to complete remaining standards of interoperability, security, privacy, and any new standards that may be proposed. HITSP and CCHIT should formalize the handoff of standards, so that there is a documented process for these standards to become certification criteria. HHS could shorten the length of time of adopting standards. HHS could also fund additional value cases to expedite adoption. The Congress could help as well, by providing incentives as soon as possible—and not waiting until 2011—in addition to requiring that any electronic health record purchased with federal dollars must be CCHIT-certified.

In general, the current structure is working. Security and privacy standards have been developed and released that can secure sensitive information; authorize and

track access; authenticate users; encrypt and anonymize data; and other key priorities.

Proposed legislation

The current governance structure is delivering the technical standards of how to secure data and protect patient privacy, but there are key policy questions that are under consideration that will drive the broader agenda. The House Energy and Commerce committee introduced legislation last week that contains a range of proposals that impact privacy and progress, and members of the United States Senate will soon debate their own proposals.

One of the most controversial issues is patient privacy. Some advocates for very strict privacy protections have outlined specific changes they support. Many in the industry have recoiled at them, as they view many of the proposed requirements as onerous, administrative nightmares. There is a middle ground. There are details to be worked out, but the following proposals include principles and policies that can be balanced to help find consensus.

Individual consent

Yes, there should be a legal framework that includes the right of individual consent. Patient consent can be balanced so that it does not impose new, undue burdens on providers, health plans, and other entities.

One way to accomplish this may be through a uniform patient consent form. Such a form could specify standards and instructions that “clearly reflect patients’ rights to information in their medical records and provider confidentiality principles.”⁷ Such a form could be collected at the time of enrollment in a public or private health plan or before services are delivered. Consumers could opt-out of certain products, services, or notifications and specify how their specific identifiable information can or cannot be shared outside the course of treatment or payment. Some questions will need to be addressed, such as what to do when consent has not been or cannot be given. The Congress should allow the regulatory process to answer such questions.

Another important balance is between identifiable information and de-identified data. We must balance consent and privacy with health services research and public health. I am a strong believer in the power of data. When medical data is turned into secure, actionable knowledge, it saves lives and saves money. Data can reveal which treatments work and those that do not; the effectiveness and relative value of drugs, devices, and medical procedures; variation in the delivery of care; who may be a good candidate for clinical trails; and other vital information that benefits all.

⁷ RTI International, *Privacy and Security Solutions for Interoperable Health Information Exchange: Assessment of Variation and Analysis of Solutions*, July 2007. http://www.rti.org/pubs/avas_execsumm.pdf (Accessed January 24, 2009.)

It is an indisputable societal benefit to generate this kind of knowledge. It delivers better health at lower cost. But it is simply impossible to do without the wide aggregation and availability of de-identified data. Because the data is de-identified, meaning that all identifiable markers are stripped away that can be traced to a specific individual, personal privacy is protected.

Additionally, there are certain services that health plans offer to their members or that health systems do on behalf of their patients that should still be made available. Disease management, chronic care management tools, and other valuable services should be recognized as treatment and not have new onerous restrictions on identifying possible enrollees or patients who would benefit from a particular medical program.

Data breach notification

Yes, patients should be notified of egregious breaches of privacy and security. We expect our banks, credit card companies, or other financial institutions to do this when our financial data is compromised. So, too, must healthcare organizations.

The standard for what defines a breach must be set very high; as there must be a balance between informing patients and burdensome reporting requirements for health plans, physicians, and other providers.

Protections should incorporate a risk-based notification, so that physicians, health plans, and health systems do not notify patients for harmless or inadvertent data sharing. If, for instance, a physician mistakenly sees the record of a patient he or she is not treating, should that qualify as a data breach? Should the patient whose record was seen be notified? The bar should be set very high so that these types of cases do not generate unnecessarily notifications.

When a notification is required, informing patients must make sense. For instance, does it make any sense that a health plan or provider who lacks updated contact information for patients whose privacy has been breached be required to post on their homepage or take out an ad in a major media outlet that the patient's privacy has been breached? No patient would want that advertised.

Enforcement

Yes, new protections will need to be enforced, and this should be done through existing offices and departments. The last thing our health system needs is more bureaucracy, such as new privacy consultants at HHS regional headquarters or a new office of health information privacy.

Patients should have a private right of action in federal court for extreme breaches of privacy. Again, there must be a balance; this time between patient privacy and creating a new legal market for frivolous lawsuits. To strike the right balance, the bar must be set very high so that federal—not state—litigation is available for patients, but only for clear, egregious cases.

Additional patient protections should be added for deliberate or extreme breaches of privacy. One step in the right direction is to dramatically toughen existing penalties. The Congress should closely examine possible changes to Title 18 of the U.S. Code of Criminal Procedures that would harshly punish the malicious use of personal health information, such as hacking into electronic medical records and publishing or posting online any personal health information. Another option would be to expand current breach-of-privacy laws to include healthcare.

Personal Health Records

Broad-based regulation of personal health records offered by non-covered entities or non-business associates is too early. Patients already have the power to choose whether or not to use such portals and many give patients total control over how their information is shared; who can access it; and if their personal health information can be used to tailor services.

The value of these kinds of products and services is clear. Personal health records and other portals can inform and educate consumers about their health and empower them to better manage their healthcare records that are currently fragmented across the system. Despite these benefits and others, consumer portals are relatively new to the market and still need time to mature. Regulation of any product that is in such a state of infancy will undoubtedly harm their growth—and in this case suffocating the growth of personal health records would rob consumers of their obvious value.

Where changes could be made are to promote “portability” within HIPAA. Consumers should have the legal authority to direct their data to third parties or CCHIT-certified technology products; consumers should have a right to standardized electronic copies of their data with near real-time compliance. These kinds of changes to existing law will not only empower and protect consumers but drive growth in the market. These ideas, as well as bringing stand-alone personal health records under HIPAA, should be studied fully.

Conclusion

We need policy solutions that properly balance privacy with progress and do not go too far in either direction. The risks of favoring one side over the other are real. If privacy protections go too far and place burdens on providers, they will not adopt new technology; and even if they do, valuable data that does not infringe upon privacy could be trapped. However, if privacy protections do not give patients true control over their personal health information or puts that information at risk, we could build the most modern system, and no one would trust it.

We do not need to make a choice between protecting privacy at all costs and making progress at any cost. We can find the right balance if we are careful, judicious, and realistic. Once we do, we will have succeeded in transforming healthcare into a system that saves lives, saves money, and protects privacy.

Appendix I

Excerpted testimony of former Speaker of the House Newt Gingrich

Founder, Center for Health Transformation

House Government Reform Committee

March 15, 2006

The Individual Owns Their Personal Health Record and All of their Health Data

With the rapid development of individual-centered health information technology such as the personal health record, the question then arises, “Who owns the data?” Doctors, hospitals, and other providers often believe that they own the encounter data because they saw the patient and collected the information. Employers and health plans often believe that they own the data because they paid for the services. Laboratory companies, pharmaceutical manufacturers, and other stakeholders often believe they own the data because they ran the tests or provided a product or service to the patient.

All are correct to some extent, but they forget that there is one constant variable running through all these scenarios: the individual. The individual owns the data, which they can then allow each stakeholder to have a copy of their data.

Individuals have the right to control—and must have the ability to control—who can access their personal health information. All health information technology should be deployed to improve individual health, not to protect the status quo of proprietary claims to data. In this case, where federal employees may decide to activate a personal health record, each stakeholder should be given equal access to the record—by the consumer—in the course of delivering care.

###

Appendix II

“Protecting Privacy and Confidentiality in the Nationwide
Health Information Network”

By Mark Rothstein

From the book *Paper Kills*

Edited by David Merritt

Published by Center for Health Transformation

Protecting Privacy and Confidentiality in the Nationwide Health Information Network

Mark A. Rothstein, J.D.*



Editor's Introduction

Information about our health and healthcare is by far the most sensitive data we own. From chronic conditions to medications to genetic makeup, our personal health information reveals intimate details about who we are, what we do, and what we may be like in the future. Thus, protecting our privacy and confidentiality is a principle that simply cannot be compromised. As the pace of modernizing healthcare quickens through health information technology, tension grows between protecting patients' personal data and having instant access to their comprehensive medical histories. On the one hand, having real-time access to personal health information—such as current medications and allergies—can often mean the difference between life and death. On the other hand, the release of such sensitive data to outsiders, especially those with nefarious or self-interested intentions, can have disastrous consequences. An interoperable, nationwide system will undoubtedly save lives and save money, and it is an absolutely essential part of transforming health. But it must be built, deployed, and adopted in a manner that ensures responsible, appropriate, and authorized use.



Privacy, including health privacy, is an intriguing concept. In the United States, virtually everyone is in favor of health privacy. But when people are confronted with the costs it entails—in inconvenience and expense—the public's support for it declines. Furthermore, there is no generally accepted definition of what health privacy actually means. For instance, the primary privacy concerns of the public

* Mr. Rothstein serves as Chair of the Subcommittee on Privacy and Confidentiality of the National Committee on Vital and Health Statistics, the federal advisory committee charged with advising the Secretary of Health and Human Services on health information policy. The views expressed in this chapter, however, are solely those of the author.

Paper Kills

regarding adoption of electronic health records (EHRs) are that irresponsible healthcare entities and rogue employees will divulge information or that snoops and hackers will get access to private information,¹ but these concerns are more properly characterized as health information security issues.

The definition of health privacy comprises at least the following four meanings: (1) informational privacy, which concerns access to personal information; (2) physical privacy, which concerns access to persons and personal spaces; (3) decisional privacy, which concerns governmental and other third-party interference with personal choices; and (4) proprietary privacy, which concerns the appropriation and ownership of interests in human personality.²

Confidentiality is closely related to privacy. It refers to the conditions surrounding a situation when information provided within a confidential relationship (e.g., physician-patient) may be disclosed to others. Confidentiality has been a cardinal principle of medical ethics since the time of Hippocrates. With confidentiality, physicians offer their patients the following arrangement: accept a lower level of control over your sensitive health information (confidentiality vs. nondisclosure), because doing so is important to your health, and your information will not be disclosed without your permission.

Privacy and confidentiality are sometimes viewed as individual rights that clash with the societal interest of disclosure of health information. In fact, society has a strong interest in protecting privacy and confidentiality because public health would be endangered if people were afraid to share sensitive information with their healthcare providers. At the same time, individuals have a strong interest in disclosure, because medical research and other social goods depend on the availability of individual health information. Thus, the costs and benefits of privacy and confidentiality need to be balanced for the benefit of both individuals and society.

The development of the Nationwide Health Information Network (NHIN) raises important questions of privacy and confidentiality. As the amount of easily accessible health information increases, so too do the potential risks to privacy and confidentiality stemming from inappropriate disclosures. Consequently, unless the public is satisfied that adequate measures are in place to protect

health information, the political viability of the NHIN will be threatened.³

Today's Protections for Health Privacy and Confidentiality

America's healthcare system protects privacy and confidentiality in three ways. First, confidentiality is a basic element of medical ethics. In 1847, the first Code of Ethics of the American Medical Association (AMA) expressly recognized the importance of confidentiality,⁴ and all subsequent versions of the AMA Code, as well as the ethical codes of nurses, dentists, pharmacists, and other health professionals, recognize the importance of confidentiality.⁵ Regardless of legal protections or health information technology, confidentiality is, in the first instance, based on the integrity and professional ethics of those who use health information in providing care.

Second, health privacy and confidentiality are protected by a patchwork of federal and state laws. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule⁶ is the closest thing to a comprehensive health privacy law, but it has limited coverage. The privacy provisions are part of a federal law addressing health claims, and therefore they apply only to health providers, health plans, and health clearinghouses that submit or pay health claims in standard electronic formats. Thus, HIPAA does not apply to employers, schools, life insurers, and other entities that routinely access, use, and disclose health information. Nor does it apply to the myriad providers who do not submit claims in electronic form. Information protected while under the custody of a covered entity loses its protected status when it is disclosed to a non-covered entity. Furthermore, there are few limits on the re-disclosure of health information to "business associates" of covered entities, including those located off-shore.

Other federal laws have even more limited applicability. For example, the federal Privacy Act⁷ applies only to health information in the possession of the federal government. Another law protects the confidentiality of substance abuse treatment information,⁸ so that illicit drug users (who are breaking the law) will seek treatment without fear of arrest. The Americans with Disabilities Act limits the types of health record disclosures permissible in the employment setting.⁹ Other laws deal with health information in biomedical research.¹⁰

Paper Kills

Several states have laws setting forth privacy and confidentiality rules for healthcare, such as the need for patient consent for disclosure of information.¹¹ Many states also have laws applicable to certain types of information, such as mental health records, genetic information and HIV/AIDS status. These laws attempt to protect what is perceived to be some of the most sensitive or stigmatizing information.

The third factor protecting the confidentiality of health information is the fragmentation of our largely paper-based health records system. As a practical matter, it would be virtually impossible to identify and aggregate all an individual's medical records, which might be stored in dozens of physicians' offices, hospitals, laboratories, and other facilities in diverse locations. Consequently, individuals can be fairly certain that the otherwise lamentable lack of coordination of their health information has the indirect effect of protecting from disclosure disparate health records that could contain sensitive information. This inadvertent protection, however, is likely to disappear with the creation of the NHIN.

Patients' Rights

A health records system that respects privacy and confidentiality should empower individuals to take an active role in deciding the proper use and disclosure of their health information. To accommodate wide choices for patients, a health record system must be flexible; but if patients have too much control over the content of health records, the records might be inadequate to provide essential information for healthcare. Thus, recognizing the importance of meaningful patient choice over aspects of their health records should not be seen as endorsing unlimited patient control.

The Right to Accept or Decline Participation in the Nationwide Health Information Network (NHIN)

The precise structure and operating mechanism of the NHIN have yet to be determined. Under any likely arrangement, however, individual electronic health records will be accessible via an interoperable network. At the very least, individuals should have the choice whether to make their health records available via the NHIN. It is not entirely clear what such a decision would mean in practical terms. For example, would it still permit the individual to elect, on a

one-time basis, to send a particular set of medical records over the NHIN? If so, then the difference between individuals whose records may be sent “automatically” over the NHIN and those whose records require a special, one-time authorization may be slight. To protect themselves, healthcare providers might require individual authorizations for each non-emergency use of the NHIN for all of their patients. The effect would be to turn all patients into potential one-time users, albeit at a high administrative cost.

The choice to participate in the NHIN is only a starting point. How are such decisions to be made? The most common way of framing the issue is to ask whether the system should be “opt-in” or “opt-out.” In the former situation, the presumption or default is that individuals are not part of the NHIN until some express action is taken to permit disclosure. In the latter, individuals could elect not to be a part of the system, but if they do nothing, their records would be accessible via the NHIN.

Although I support the opt-in approach because it is consistent with numerous other aspects of informed consent in healthcare, in practice, there may be little difference between opt-in and opt-out. An analogous debate arose and continues to exist over the HIPAA Privacy Rule. The original proposed rule required that individuals consent to have their protected health information used and disclosed for treatment, payment, and healthcare operations.¹² The final, revised rule withdrew the requirement of consent; instead, it simply mandates that all covered entities provide a notice of privacy practices to individuals, and covered entities with a direct treatment relationship must make a good faith effort to obtain a signed acknowledgment from the individual of receipt of the notice.¹³ In practice, patients are usually asked to sign the acknowledgment without any explanation of what it is and often without even receiving the notice. In this environment, replacing the acknowledgment with a consent form would make no difference to most patients, as they would merely be asked to sign a different HIPAA form, with no further explanation.

Based on the unsatisfactory experience with the HIPAA Privacy Rule’s approach to notices and acknowledgments, it is imperative that executing an NHIN opt-in or opt-out document be more meaningful. Patients need understandable, culturally appropriate

Paper Kills

information about the significance of their choices. Because settings such as a hospital admissions desk and a physician's office reception area are not the best educational environments, broader public education is needed. No such program was ever implemented for the Privacy Rule, and the experience strongly suggests that unless the NHIN contains a substantial educational component, any process whereby patients indicate their decision about participating in it is likely to be deeply flawed.

The Right to Control the Contents of Records Disclosed via the NHIN

Many (or perhaps most) people are not bothered by the release of "routine" elements of their health records. They are only troubled by the prospect of disclosing the most sensitive material. For example, one study at a major medical center involved 100 individuals from each of the following six disease groups: cystic fibrosis, sickle cell disease, diabetes, HIV infection, breast cancer, and colon cancer.¹⁴ When asked whether special privacy protections should be in place for certain medical conditions, they indicated the following conditions as most in need of special protection (in order of need): abortion history, mental health history, HIV/AIDS, genetic test results, drug/alcohol history, and sexually transmitted disease. Assuming that individuals have the right to choose whether to have their records disclosed via the NHIN, if they lack the ability to designate certain information for nondisclosure, then they will simply decline to be part of the NHIN. Thus, some degree of specificity regarding the records to be disclosed is essential to maximize participation in the NHIN.

It may be difficult to determine the appropriate level of patient control over their health records. If patients have too little control, they might decline to have their records accessible via the NHIN; but giving them too much control might not be a good idea, either. For example, if patients had the right to select *any* items in their health records for nondisclosure via the NHIN, then healthcare providers receiving the records would be unsure as to what items could have been removed. To be safe, many providers might obtain a complete medical history for each new patient, thereby eliminating a primary benefit of the NHIN.

One way of giving patients an appropriate degree of control over their information disclosed via the NHIN would be to establish standard information fields that could be selected by patients for

nondisclosure. Such criteria might be based on the age of the information (e.g., items over ten years old), the type of information (e.g., mental health, substance abuse), the type of provider (e.g., psychiatrist), or other bases. If both patients and providers know the rules of disclosure, then privacy could be protected without the need for taking new comprehensive histories. Physicians might inquire, for example, if information from an “optional” field might affect diagnosis or treatment.

One strategy for implementing the approach of selective nondisclosure is the use of “blocking.” Patients could designate certain areas of their records to be blocked from disclosure to all or a subset of their healthcare providers. Nevertheless, even if information is blocked, computerized decision support could still scan blocked information to protect patient safety.

If a patient, for example, is taking medication for a psychiatric condition, and the diagnosis and medication are blocked, the decision support would still check for a possible drug interaction between the blocked medication and a new medication under consideration by the physician. If so, then the physician would receive a message about a drug interaction with a blocked prescription. The physician then could prescribe another medication, obtain information from the patient about the blocked medication, or take other steps. Blocking with decision support is likely to improve patient safety over current prescribing practices, wherein patients often get a second prescription without mentioning the first prescription to their physician.

The Right to Control the Contents of Local Health Records

Focusing attention exclusively on health records as they are transmitted via the NHIN is too narrow. For one thing, in the architecture of the NHIN (or some future version of it), any distinctions between “local” records and “network” records may dissipate. Second, patients may not recognize a distinction between the two aspects of their health records. Thus, the question arises as to whether patient controls over health records should apply to local health records and, if so, how should it be done.

I see no reason why patients should not be able to control aspects of their health records regardless of the location or designation of the status of the records. The privacy interests of patients are

Paper Kills

the same, and the practicalities are often the same. For example, in a large, integrated health delivery system, the scope of actual or potential disclosures within the system (not using the NHIN) will exceed the disclosures made via the NHIN from a sole provider to another sole provider.

One way to reduce the scope of disclosure is the use of role-based access criteria, under which the level of access of any healthcare provider within a healthcare institution depends on the role and needs of the individual. Thus, treating physicians and nurses would get a higher level of access than billing clerks and food service workers. Role-based access criteria already have been adopted by many large healthcare organizations with EHR systems, and this requirement should be expressly mandated for all healthcare records systems.

An extremely contentious issue involves destruction of sensitive health records. Should individuals have the right to delete certain information from their files? As noted earlier, in a largely paper-based system, individual privacy with regard to old, sensitive health information is protected because the records tend to “disappear” with age—based on patient relocation, provider retirement, storage issues, or similar factors. In an age of electronic health records, nothing will disappear, and the protections of blocking, role-based access, or other measures will not necessarily relieve the anxiety of individuals who know that embarrassing information is in their health records.

Some physicians strongly object to the concept of patients deleting certain aspects of their medical records and assert that doing so would be unethical, illegal, or would jeopardize patient care. All these arguments are related, but none are persuasive. To begin with, medical records are obtained and retained for the benefit of the patient, and laws or professional standards limiting alteration or destruction of records are for the benefit of the patient. The AMA Code of Medical Ethics provides:

Physicians have an obligation to retain patient records which may reasonably be of value to a patient. . . . Medical considerations are the primary basis for deciding how long to retain medical records. For example, operative notes and chemotherapy records should always be part of the patient’s chart. In deciding whether to keep certain parts of the record, an appropriate

criterion is whether a physician would want the information if he or she were seeing the patient for the first time.¹⁵

This provision is instructive because it indicates that it is permissible for certain parts of a patient's record to be destroyed, that medical considerations govern how long records information should be kept, and that benefit to the patient is the overriding purpose of maintaining the records.

There are many examples of sensitive health information in medical files with no continued clinical relevance. Here are two examples:

(1) A 25-year-old woman comes to the emergency department of a local hospital with bruises and minor lacerations as a result of being abused by her boyfriend. She is treated and released. She promptly breaks up with her boyfriend. Twenty years later, she is happily married to another man and has two healthy children. Does her report of abuse at the hands of her old boyfriend need to remain in her file?

(2) A 25-year-old graduate student celebrates the end of exams with an evening of excessive drinking and carousing, which ends with a liaison with a commercial sex worker. A week later, concerned about the health implications of the adventure, he has his physician run a battery of tests for sexually transmitted diseases. All the tests are negative and the carousing is not repeated. Does the record of sexually transmitted disease testing, and the reason for it, need to remain in his file for the rest of his life?

I would argue that deleting sensitive health information under some appropriate standards and procedures would be ethical, not jeopardize patient health, and would support public health by not discouraging individuals from seeking care in sensitive situations. To the extent that removing certain information is unlawful, which the AMA asserts is not usually the case,¹⁶ applicable laws should be amended or repealed.

The Right to Know Disclosures Beyond Healthcare

The loss of health privacy creates a substantial risk of tangible harm to individuals. Ironically, the disclosures leading to these harms are almost always lawful. In the United States, laws to protect health

Paper Kills

privacy are designed to protect against unauthorized access to, use of, and disclosure of personal health information. Few laws place any restrictions on the scope of information that third parties may require individuals to disclose pursuant to an authorization. Individuals need not sign an authorization to release their health records, but if they refuse, they will not be considered for employment, life insurance, or other essential transactions or opportunities. Furthermore, disclosures of health records pursuant to an authorization tend to comprise the entire record, regardless of any limitations listed in the authorization.

Few people realize the pervasiveness of compelled authorizations. In a recent article, Meghan Talbott and I estimated the number of compelled authorizations each year in the United States at 25 million.¹⁷ The list of uses includes health information disclosed for employment entrance examinations, individual health insurance applications, individual life insurance applications, individual long-term care insurance applications, individual disability insurance applications, individual and group disability insurance claims, automobile insurance personal injury claims, Social Security Disability Insurance applications, workers' compensation claims, veterans' disability claims, and personal injury lawsuits. It is impossible to protect health privacy and confidentiality without regulating compelled disclosures of health information.

Although it is often necessary for third parties to consider an individual's health information in each of the uses described above, it is rarely necessary to consider an individual's entire health record. Moreover, with the advent of the NHIN, the amount of information accessible about each individual will increase dramatically. Thus, it is likely that more sensitive health information of no relevance to a non-healthcare use might be routinely disclosed millions of times each year.

Contextual access criteria are computer software programs or algorithms that enable the holders of health information to limit the scope of the disclosures.¹⁸ For example, using this technique, life insurance companies would receive only information related to mortality risk and employers would receive only information related to the individual's ability to perform a specific job. It will be a challenge to develop the criteria for each of the common, non-medical uses of

health information and then to develop the programs to isolate these data fields in electronic health records. It will also be a challenge to garner the political support to restrict the scope of disclosures. Nevertheless, research efforts to develop the technology of contextual access criteria must be undertaken immediately. If the NHIN goes forward without the architecture to support contextual access criteria, it may be impossible or prohibitively expensive to add this feature later.

Nonclinical Uses of the NHIN

A network of interoperable, longitudinal, comprehensive EHRs has many potential applications beyond promoting efficient, effective, and safe clinical care for individuals. The data derived from aggregation of individual health information would provide a rich resource for epidemiology, outcomes research, population health statistics, health quality research, healthcare utilization review, and fraud investigation. Currently, the most aggressive non-clinical use of the NHIN being developed is for real-time biosurveillance, involving natural (e.g., influenza) and man-made (e.g., bioterrorism) health threats.

Although national security is an area of great public concern, using biosurveillance as a prominent initial application of the NHIN raises significant issues. Even if privacy and confidentiality were well protected in a biosurveillance system, an emphasis on this issue might lead members of the public to question the veracity of official pronouncements that the NHIN is being created primarily to improve personal health. Before establishing a national biosurveillance system using the NHIN, five considerations need to be addressed and satisfactorily resolved.

First, public officials need to make a compelling case regarding both the need for and efficacy of such a new system. Pilot projects and smaller start-up measures should be undertaken before the NHIN is used.

Second, the measures used by the system should be the least intrusive possible. The minimum amount of data should be released to the fewest number of people in the least identifiable form.

Third, there should be transparency in establishing the system,

Paper Kills

and all stakeholders (e.g., state and local public health officials, healthcare providers, members of the public) should have an opportunity to participate in its design. To date, there has been little notice and even less public participation.

Fourth, public and professional education about the objectives, operations, and safeguards of the system is essential.

Fifth, there should be an ongoing program of independent oversight, assessment, and research to ascertain whether the system is meeting its goals and adequately protecting privacy and confidentiality.

Conclusion

The NHIN is different from other large health database projects because it is intended to facilitate the dissemination of clinical data. The participants in the NHIN are not volunteer research subjects. They are patients in clinical settings who have done nothing to enroll in the NHIN except to enter the healthcare system.

Given this framework, it is clear that the developers of the NHIN have a substantial ethical responsibility not to harm the interests of patients, and to protect their privacy and confidentiality. The interests of patients must take precedence over other intended uses of the system. There must be public participation in the system's design and a well-financed, vigorous public education program before the NHIN goes into effect. Fair information practices, such as accounting for disclosures and a complaint resolution process, should be incorporated into the NHIN. Individuals should have the right to choose whether to participate and, if they do, they should have some control over the content of the health information disclosed. Contextual access criteria to limit the scope of information disclosed to third parties for non-medical purposes should be part of the architecture of the NHIN. Strong enforcement is needed and there should be an ongoing program of research to assess the effects of the NHIN and its privacy measures.

If the preceding list seems long, difficult, and expensive—it is. Privacy and confidentiality are not cheap, and they are not easy. These protections, however, are crucial in establishing and maintaining public trust in the NHIN and its component parts. To do less

would risk losing public confidence in the entire healthcare system and exposing individuals to a range of tangible and intangible harms.

— — —

Mark A. Rothstein, J.D., holds the Herbert F. Boehl Chair of Law and Medicine and is Director of the Institute for Bioethics, Health Policy, and Law at the University of Louisville School of Medicine. Professor Rothstein is a leading authority on the ethical, legal, and social implications of genetics, privacy, occupational health, employment law, and public health law. He is Chair of the Subcommittee on Privacy and Confidentiality of the National Committee on Vital and Health Statistics, the statutory advisory committee to the Secretary of Health and Human Services on health information policy, including the privacy regulations of the Health Insurance Portability and Accountability Act. He is the immediate past President of the American Society of Law, Medicine and Ethics. He is the author or editor of 19 books. His latest book is entitled *Genetics: Ethics, Law and Policy*. He received his B.A. from the University of Pittsburgh and his J.D. from Georgetown University.

— — —

¹ Harris Interactive, "Health Information Privacy (HIPAA) Notices Have Improved Public's Confidence That Their Medical Information Is Being Handled Properly," news release, February 24, 2005. Available at <http://www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=893> (accessed March 30, 2007).

² Anita L. Allen, "Genetic Privacy: Emerging Concepts and Values," in *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era*, ed. Mark A. Rothstein (New Haven, CT: Yale University Press, 1997), 31-59.

³ National Committee on Vital and Health Statistics, Letter to Health and Human Services Secretary Mike Leavitt, June 26, 2006. Available at <http://www.ncvhs.hhs.gov/060622lt.htm> (accessed March 23, 2007).

⁴ American Medical Association, *Code of Medical Ethics of the American Medical Association*, art. I, § 2, 93 (1847). Available at <http://www.ama-assn.org/ama/upload/mm/369/1847code.pdf> (accessed March 30, 2007).

⁵ Rena A. Gorlin, ed., *Codes of Professional Responsibility: Standards in Business, Health and Law*, 4th ed. (Washington, D.C.: BNA Books, 1999).

⁶ 45 C.F.R. Parts 160, 164 (2004).

⁷ 5 U.S.C. § 552a (2000).

⁸ 42 C.F.R. Part 2 (2004).

⁹ 42 U.S.C. § 12112(d) (2000).

¹⁰ 45 C.F.R. Part 46 (2004).

¹¹ Joy Pritts et al., *The State of Health Policy: A Survey of State Health Privacy Statutes*, 2nd ed. (Washington, D.C.: Georgetown University Press, 2002). Available at

Paper Kills

<http://hpi.georgetown.edu/privacy/pdfs/statereport1.pdf> (accessed March 30, 2007).

¹² Department of Health and Human Services, "Standards for Privacy of Individually Identifiable Health Information," *Federal Register* 65, no. 250 (December 28, 2000): 82,462-829 (proposed section 164.506(a)).

¹³ 45 C.F.R. § 164.520 (c)(2)(ii).

¹⁴ Laura Plantinga et al., "Disclosure, Confidentiality, and Families: Experiences and Attitudes of Those With Genetic versus Nongenetic Medical Conditions," *American Journal of Medical Genetics* 119C, no. 1 (2003): 51.

¹⁵ American Medical Association, Code of Medical Ethics § 7.05: Retention of Medical Records (2006-2007 ed.) (2006).

¹⁶ *Ibid.*

¹⁷ Mark A. Rothstein and Meghan K. Talbot, "Compelled Authorizations for Disclosures of Health Records: Magnitude and Implications," *American Journal of Bioethics* 7, no. 3 (2007): 38-45.

¹⁸ Mark A. Rothstein and Meghan K. Talbot, "Compelled Disclosures of Health Information: Protecting against the Greatest Potential Threat to Privacy," *Journal of the American Medical Association* 295 (2006): 2882-85.



Statement for the Hearing on:

**“Health IT: Protecting Americans’ Privacy in the Digital
Age”**

U.S. Senate

Committee on the Judiciary

Tuesday, January 27, 2009

National Association of Chain Drug Stores

**413 N. Lee St. Alexandria, VA 22314
(703) 549-3001
www.nacds.org**

Mr. Chairman and members of the Committee, the National Association of Chain Drug Stores (NACDS) is pleased to submit a statement for the record on protecting Americans' privacy with respect to health information technology (HIT). NACDS supports the passage of federal health information technology HIT legislation. More importantly, we are pleased to assure you that pharmacists and pharmacies have taken significant steps, consistent with HIPAA regulations, and state laws and regulations, to safeguard our patients' data. We take a back seat to no one in our commitment to protecting sensitive patient information. We commend you for holding this important hearing.

The National Association of Chain Drug Stores (NACDS) represents traditional drug stores, supermarkets, and mass merchants with pharmacies. Its more than 170 chain member companies include regional chains with a minimum of four stores to national companies. NACDS members also include more than 1,000 suppliers of pharmacy and front-end products, and nearly 90 international members representing 29 countries. Chains operate more than 39,000 pharmacies, and employ a total of more than 2.5 million employees, including 118,000 pharmacists. They fill more than 2.5 billion prescriptions yearly, and have annual sales of over \$750 billion.

Chain Pharmacy's Leadership Role in HIT Adoption

Chain pharmacy has been on the leading edge of the adoption of HIT for many years. We have been actively involved in fostering the use of technology to improve the quality of patient care and developing standards to allow the exponential growth of HIT in pharmacy practice. For example, pharmacy computer health information systems provide pharmacists with information on the patient's prescribed drugs, potential drug to drug interactions, and drug dosing. Pharmacy HIT systems also assist pharmacy with other aspects of pharmacy patient care services such as medication therapy management and evaluation of a patient's compliance and adherence to the prescribed drug therapy regimen.

Another example of how chain pharmacies have fostered adoption of HIT is electronic prescribing. Today, most pharmacies in the United States have the capability to receive electronic prescriptions. More than 95% of the nation's retail community pharmacies have tested and certified their pharmacy applications through SureScripts-RxHub. Chain pharmacy supports the widespread adoption of electronic prescribing technology in the health care community as evidenced by our creation of SureScripts. NACDS and the National Community Pharmacists Association (NCPA) created SureScripts in 2001 as the foundation for an electronic prescribing network. Their mission was to improve the overall prescribing process and to ensure, among other things, neutrality, patient safety, privacy and security, and freedom of a patient's choice of pharmacy and physician's choice of therapy. Under the leadership, and with the backing of the chain pharmacy industry, SureScripts created an open, neutral, and secure information system, known as the Pharmacy Health Information Exchange, which is compatible with all major physician and pharmacy software systems.

We believe that widespread adoption of electronic prescribing is the most critical prerequisite for the adoption of electronic medical records and other forms of HIT. Electronic prescribing technology connects physicians and other prescribers with pharmacies and health plans to streamline the delivery of patient care. The numerous benefits of electronic prescribing are well-established, including:

NACDS Statement for the record for Senate Judiciary Hearing
January 27, 2009
Page 2 of 7

- Prescribers have real-time access to formulary information, so the most effective and cost-effective medications are prescribed;
- Prescribers have real-time access to patient medication histories, so contradictory and duplicate therapies are avoided;
- Patient compliance is enhanced, as patient convenience is increased;
- Illegible or incomplete prescriptions are eliminated; and
- Direct access between prescriber and pharmacist allows for two-way communications and consultations.

Prescriber adoption of electronic prescribing creates electronic medication records within the medical practice. This introduces prescribers to the concept of electronic records; the medical record grows from here. As prescribers rely more on electronic records, they become more comfortable with them and will seek to have more patient information available electronically.

Drug Enforcement Administration (DEA) Remains an Obstacle

However, a major obstacle to widespread prescriber adoption of electronic prescribing is the current Drug Enforcement Administration (DEA) prohibition on electronic prescribing of controlled substances, which comprise approximately 15-20% of all prescriptions. Prescribers are reluctant to adopt electronic prescribing technologies until they can issue all prescriptions electronically, not just ones for non-controlled substances. DEA has proposed regulations to allow the electronic prescribing of controlled substances, but prescribers, pharmacies and other health care providers have strong concerns that the proposed rules are not workable. Electronic prescribing will not become widespread until DEA issues workable regulations.

Ensure Continued Pharmacy Involvement

We agree with President Obama that the provision of financial resources is necessary to foster widespread HIT adoption. As the most consumer-accessible health care provider, pharmacy's critical role should be recognized in the development of an interoperable healthcare delivery system. As such, pharmacies should be considered for any grant or incentive funding that fosters further adoption of HIT. For example, access to information in electronic medical records is vital for pharmacists to help manage the care of their patients. Pharmacies should be given the resources to participate in the development and adoption of these records. Similarly, we urge inclusion of pharmacists in the various standard setting and policymaking bodies that will be created or maintained by HIT legislation.

Privacy Provisions Require More Consideration

As Congress moves to foster the adoption of HIT, chain pharmacy strongly believes that these efforts must not be thwarted by requirements that are disincentives to its adoption. An appropriate balance between privacy protections for patient health information and allowing healthcare practitioners to provide patient care services and engage in healthcare operations is essential. Unnecessary burdens will have a detrimental impact on pharmacists and other healthcare providers by requiring them to spend their valuable time on administrative activities, rather than on patient care services.

We believe the HIPAA Privacy and Security Rules establish an appropriate balance with well-reasoned standards for the protection and security of personal healthcare information. Both rules

NACDS Statement for the record for Senate Judiciary Hearing
January 27, 2009
Page 3 of 7

received significant scrutiny at a national level, and we question the need for additional laws and regulations other than adding entities not currently considered covered entities. We are supportive, however, of evaluating current federal privacy and security standards and understanding the benefits of promoting and not impeding the adoption of HIT.

Let us be clear: chain pharmacy is committed to protecting patient privacy. As health providers, this is our obligation. And, as businesses, if pharmacies violate our patients' trust, we will pay a price in the marketplace. But forcing us to adopt costly and administratively burdensome privacy requirements will hurt our ability to serve patients in a timely and effective manner. Our concerns include requirements for healthcare providers to track and store a detailed record concerning how health information is disclosed for routine purposes, requirements for prior authorization for communications to patients about healthcare treatment, requirements to notify patients about innocuous and incidental breaches, and new enforcement mechanisms.

Consensus has yet to be reached among all relevant stakeholders on how best to address complex privacy issues. Consequently, we believe it would be premature or even ill advised for Congress to attempt to legislate at this time in this an area that remains highly contentious. However, if Congress continues to pursue changes to the HIPAA Privacy Rules, we believe Congress should take the path of directing the Secretary of HHS to engage in *negotiated rulemaking* instead of enacting substantive legislation on these issues.

In negotiated rulemaking, a representative group of stakeholders and a federal agency meet to negotiate the text of a proposed rule with the goal of reaching consensus on the terms of the rule before it is published for public notice and comment. Drafting a rule through negotiated rulemaking works best to thoroughly air all concerns and resolve difficult issues, such as the issues that must be addressed to assure the privacy of protected health information (PHI), while assuring its use in the provision of patient care and the improvement of that care over time.

Having stakeholders meet to draft regulations in a negotiated process would result in regulations that better meet the needs of affected interests. Negotiated rulemaking would provide the government and affected parties the time and opportunity to hear and consider each others concerns on these complex issues.

Our primary goal is for legislation not to interfere with pharmacies' ability to provide the communications necessary to ensure high quality patient care, while assuring protections for PHI. We have seen many provisions in federal legislation that would be operationally difficult and costly, more so for pharmacies than other health care providers. Pharmacies are ahead of other health care providers in the adoption of health care technology. We should not be penalized for our leadership in this area. Policymakers should focus on legislation that helps health providers and healthcare businesses be more cost effective and efficient so they can concentrate on patient care activities. Our specific concerns with provisions we have seen in federal legislation are provided in more detail below:

Accounting of Disclosures

The economic stimulus legislation moving through the House of Representatives would expand the HIPAA accounting of disclosures requirement to all disclosures made through an electronic

health record (EHR). We are concerned that many covered entities, including pharmacies, have no way to obtain information about the disclosures of business associates. This provision would require covered entities and business associates to completely redesign their information systems to be able to capture and share this information with each other.

Moreover, pharmacies make thousands of disclosures every day in order to process claims for payment and provide health care. Our information systems have not been designed to comply with this type of requirement for the billions of transactions that would be required to be recorded and stored for a minimum of three years. Pharmacies may be forced to scrap existing pharmacy systems for brand new systems that would comply with the mandate. This would be costly and could be disruptive to the timely delivery of care. The requirements would overwhelm existing systems.

Instead of expanding the accounting of disclosures, NACDS seeks a provision that would require a covered entity to provide to a patient, upon request, a listing of examples to whom it discloses PHI for payment, treatment, and operations purposes. This would provide patients who are interested in an accounting of disclosures with the necessary information to illustrate to them with whom the pharmacy will disclose their information. Most of the disclosures made for treatment, payment, and operations are recognized as routine disclosures under the HIPAA privacy rules. As such, the same disclosures to the same entities occur repeatedly. We see little value in tracking and maintaining detailed information about all these repeated transactions.

Finally, we believe the vast majority of patients would be in agreement with our proposal, as few patients have sought accounting of disclosures. The few patients who seek more details could talk with the pharmacist or corporate headquarters for more information.

Marketing Issues

The economic stimulus legislation moving through the House of Representatives would prohibit pharmacies from receiving payment for communications to patients without a HIPAA authorization. Since pharmacies cannot continue to provide these communications without proper payment, this creates an "opt-in" requirement for patient communications. Consumers rarely opt-in to receiving communications; consequently, patients would be unaware that they could be receiving beneficial communications from their health care providers. These are communications that benefit not only patients' health and wellness, but also overall public health and health care delivery costs.

We greatly appreciate an amendment offered by Representative Blunt, and adopted unanimously by the House Energy and Commerce Committee last week, which recognizes the importance of these pharmacy communications. This amendment helps continue the dialogue toward achieving legislative language that preserves these communications while addressing any privacy concerns.

This HIPAA authorization requirement is a much more complex and burdensome process than obtaining patient consent. An authorization is a detailed, customized document that gives the covered entity permission to use or disclose specified PHI for particular purposes. An authorization covers only the uses and disclosures and only the PHI addressed in the authorization. One authorization may not be used for more than one purpose, must have an

NACDS Statement for the record for Senate Judiciary Hearing
January 27, 2009
Page 5 of 7

expiration date, and a patient may revoke it at any time. The authorization must state who may use and disclose PHI and who may receive PHI. We cannot develop customized authorizations for each patient, and we cannot rely on authorizations that may be revoked at any time.

NACDS supports changes that would exempt from the definition of “marketing” all health-related communications. These communications are treatment activities that save money and lives by urging patients to follow their doctors’ prescriptions, such as prescription refill reminders. This provision would worsen prescription noncompliance – which is estimated to cost \$177 billion annually in direct and indirect healthcare and economic costs. This language would also stop communications to patients that help them better understand their health conditions and preventative care, and obtain optimal results from their treatments, such as those that educate patients about their conditions, medications, and new and alternative treatment options. These important communications empower patients to communicate more effectively with their health care providers and reinforce treatment regimens.

In addition to providing information to patients, these communications also notify patients about health and wellness programs that they should consider participation in, such as:

- Medication therapy management: programs in which pharmacists review patients’ medication profiles for possible interactions, duplication of therapies, and harmful side effects.
- Disease management programs: programs in which pharmacists work with patients with chronic diseases (e.g. diabetes, asthma, hypertension, heart disease) to ensure that they are following advice that allows them to live longer and healthier lives.
- Immunization clinics: scheduled clinics in which pharmacists provide convenient, low-cost immunizations for influenza, shingles, pneumonia, and other diseases that disproportionately affect the elderly and chronically ill.

These communications also educate patients about the cost saving benefits of generic medications. Generic medications provide the same therapy, and can do that at a fraction of the cost of their brand-name counterparts.

We urge Congress to consider the unintended consequences to public health that could result from this provision. Pharmacies offer numerous beneficial services through the communications that would be hindered by this provision.

Breach Notification

The economic stimulus legislation moving through the House of Representatives would implement complex breach notification provisions. Without an objective standard for when breach notification must occur, patients would be overwhelmed with confusing and notices for disclosures that are not meaningful.

We support language that ensures individuals would have a right to be notified by a covered entity if that covered entity *wrongfully discloses PHI and such wrongful disclosure is materially expected to result in medical fraud or identity theft*. This would ensure that patients only receive notification when there is a risk for material harm; otherwise, patients could disregard notification of a potentially significant event after receiving multiple notifications for trivial or

inconsequential events. We believe this type of standard would match the intent of the bill by only requiring alerts for unsecured information. Furthermore, requiring notification or posting of breaches to local media or HHS, based on the number of individuals affected, and not the potential for harm created, may improperly exaggerate the severity of any given breach.

In the alternative, we support the breach notification requirements found in the version of the "Wired for Health Care Quality Act" of the 110th Congress (S. 1693) that was expedited for Senate consideration through attempted unanimous consent last summer. This version tasked the Secretary of HHS with developing breach notification requirements through rulemaking.

State Attorney General Enforcement

The economic stimulus legislation moving through the House of Representatives would provide state attorneys general with the ability to bring civil actions in federal court to enforce the HIPAA rules.

This is unnecessary since the federal government (HHS) already has enforcement powers under HIPAA. States also already have enforcement powers under state privacy laws. We fear this would lead to inconsistent and inequitable outcomes. Currently, enforcement exists under the authority of HHS. If individuals and states can bring actions in different district courts, it may lead to different interpretations. Moreover, this has the potential to result in a multiplicity of civil actions for the same incident and lead to costly and unnecessary litigation expenses. This is contrary to the legislative intent that HIPAA enforcement should be aimed at encouraging ongoing compliance and not punitive actions.

New, Higher Penalties

The economic stimulus legislation moving through the House of Representatives would impose new, higher penalties for violations. Rather than imposing new penalties, we recommend a requirement for a study to look at privacy violations. At this time, it is not known if many HIPAA violations are occurring; we should not assume that a problem exists. We believe that more resources should be given to Office for Civil Rights (OCR) for enforcement and compliance activities, and then increase penalties if it is found that the existing penalties are not adequate.

Conclusion

Chain pharmacy remains committed to working with Congress to foster widespread adoption of HIT with an appropriate balance between protections for patient health information and the delivery of pharmacy and other healthcare services to patients. We believe it is critical to foster HIT adoption without attaching provisions in the name of privacy that would actually frustrate the goals of HIT adoption. We ask Congress to consider delegating privacy-related provisions to the Secretary of HHS for negotiated rulemaking; or, in the alternative to reconsider many of the privacy-related provisions that Congress is currently considering.

We thank you for the opportunity to present our views.



**National
Business
Group on
Health**

50 F Street, NW, Suite 600
Washington, D.C. 20001
202.628.9320 • Fax 202.628.9244
www.businessgrouphealth.org

Creative Health Benefits Solutions for Today. Strong Policy for Tomorrow

January 27, 2009

The Honorable Patrick Leahy
Chair
Committee on the Judiciary
U.S. Senate
244 Dirksen SOB
Washington, DC 20510

The Honorable Arlen Specter
Ranking Member
Committee on the Judiciary
U.S. Senate
152 Dirksen SOB
Washington, DC 20510

Dear Chairman Leahy and Ranking Member Specter:

As the Committee prepares for its January 27th hearing, "Health IT: Protecting Americans' Privacy in the Digital Age," the National Business Group on Health writes to re-iterate our position that extending the Health Insurance Portability and Accountability Act (HIPAA) privacy and security standards to the use of electronic personal health information (PHI) is sufficient to protect patient privacy. We are very concerned that expanding privacy and security standards that further restrict or go beyond HIPAA will hinder the ability to reap the full quality and efficiency potential of health information technology (HIT). For the past decade, the HIPAA standard has provided a workable framework for patients, physicians, hospitals, other providers, health plans and employers. The Committee, Congress and the Administration should reject any efforts to toss the HIPAA framework aside or to delay passage of the health information technology provisions in the economic recovery package.

The National Business Group on Health is the only national organization that represents approximately 300 large employers exclusively on health care and health benefits issues—including 64 of the Fortune 100—that provide health care coverage to over 55 million U.S. employees, retirees, and their families.

The National Business Group on Health applauds the new Administration and Congress for seeking to make expanded use of HIT a top priority in the economic stimulus package. We believe the United States urgently needs a nationwide electronic health-information infrastructure to enable all of us to streamline and modernize the nation's health care delivery system. Effective use of HIT, with the required business process redesign, by hospitals and physicians will improve safety, promote quality and make health care more efficient. HIT has the potential to help reduce wasteful spending and increase the value of our dollars spent on health care for the federal and state governments, employers, and patients.

The National Business Group on Health believes that assuring patient privacy is a critical component of expanded use of HIT, but that privacy and security can and should be appropriately balanced with the need to promote safety encourage medical research and save lives. This balance can be struck if we take a 21st century approach that both protects privacy and allows the sharing of information to improve quality. HIT efforts

NATIONAL BUSINESS GROUP ON HEALTH

should use sound network design—using secure open network web standards, decentralizing data, and keeping it as close as possible to where it's captured, and shared only as needed. Efforts to extend privacy provisions beyond the existing HIPAA standard are not necessary and will inhibit realization of the full potential of HIT.

Thank you for the opportunity to re-iterate our views on the importance of HIT to effective and efficient care and the extension of HIPAA's privacy and security standards to the use of electronic PHI for the Committee's Hearing on "Health IT: Protecting Americans' Privacy in the Digital Age." Please, contact me or Steven Wojcik, the Business Group's Vice President of Public Policy at (202) 585-1812 if you would like to discuss any of these comments or recommendations in more detail.

Sincerely,



Helen Darling
President

patientprivacyrights

January 25, 2009

Honorable Patrick Leahy
Chairman
United States Senate
Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

Written Testimony of Deborah C. Peel, MD and Ashley Katz, MSW, Patient Privacy Rights
Senate Judiciary Hearing: *Health IT: Protecting Americans' Privacy in the Digital Age*
January 27, 2009

Chairman Leahy and members:

Thank you for the opportunity to submit written testimony for this important hearing on health IT and privacy. Mr. Chairman, throughout your public service you have been a champion and protector of Americans' privacy rights. We applaud your dedication to this issue. The need for your privacy leadership has never been greater than it is now. As Congress implements electronic medical records and a national system to share personal health information the need to protect our privacy exponentially increases. The electronic health system must protect Americans' jobs, reputations and opportunities by ensuring that our most intimate information, our health records, are only used to improve health. The renewed commitment in Congress to protecting consumers paves the way for important privacy protections to be enacted into statute. These protections, many of which are in the Health Information Technology for Economic and Clinical Health Act" or the "HITECH Act", are the lynchpin to ensuring the President's vision for health information technology is successful.

We outline a number of specific recommendations below. **Let us highlight our key recommendation, by far the most important -- we must prohibit the sale of any electronic medical records or personally identifiable health information gleaned from the healthcare system.** It is critical to put a stop to current data sales and misuse, but also to prevent the development of future businesses that sell personal health information, treating that information as a typical commodity while doing nothing to improve Americans' health.

As the nation's health privacy watchdog, Patient Privacy Rights (PPR) works to ensure that we do not have to choose between privacy and health care or health IT. PPR is a 501(c)3 nonprofit headquartered in Austin, Texas with an office in Washington D.C., funded solely by consumers. We lead the Coalition for Patient Privacy, a diverse, bi-partisan group of consumer organizations that represents millions of Americans, including patients, doctors, disease groups, civil liberties advocates, disability groups, social workers, privacy advocates, unions, democrats, republicans, libertarians and independents. The Coalition shares one common goal: to ensure that America's health IT system protects our health, jobs and privacy. We want to innovate and improve health care in our country, but that can only be done if citizens' rights to privacy are respected.

THE NEED FOR PRIVACY

Privacy is required for health IT to succeed. Without privacy, our system will crash like any computer system with a persistent and chronic virus. Americans will not participate in an electronic health record system or worse, avoid care altogether and undoubtedly misrepresent their medical histories. By taking steps to protect individuals, the tremendous opportunities health IT offers, and the laudable goals set by the Obama administration, can become a reality. As you know, we can have both health IT and privacy. To choose between either is a false choice. Privacy enables adoption and acceptance of health IT and is essential for a quality healthcare system.

Mr. Chairman, you have consistently been ahead of the curve on the need to protect Americans' fundamental right to privacy. Eight years ago in your Report Card on Privacy you remarked:

The digitalization of information and the explosion in the growth of computing and electronic networking offer tremendous potential benefits to the way Americans live, work, conduct commerce, and interact with their government. Yet new technologies, new communications media, and new business services created with the best of intentions and highest of expectations challenge our ability to keep our lives to ourselves, and to live, work and think without having personal information about us collected and disseminated without our knowledge or consent. **Indeed, personal information has become a valuable and widely traded commodity by both government and private sector entities, which may use the information for purposes entirely unrelated to its initial collection. Moreover, this information may be stolen,**

sold or mishandled and find its way into the wrong hands with push of a button or click of a mouse.¹ (emphasis added)

Mr. Chairman, you have long foretold of the vast growth of the data brokerage and data aggregation industries. *Your privacy concerns in 2000 could not be more accurate or cogent in 2009.* Today our most intimate information, our personal health records, is one of the hottest, most sought after commodities in the market. You, Mr. Chairman, have an opportunity to take the first real action to halt data brokers' unethical and invasive practices and protect our privacy. The comprehensive protections detailed in your bill addressing the mining of data by data brokers, S. 495, can serve as an excellent model for the kinds of protections and restrictions needed for electronic medical records. Ensuring consumer protections are included as part of any legislation advancing health information technology is essential to assuring Americans will trust electronic health records and to stop the erosion of our fundamental rights to privacy. Americans support these practical, common sense protections for health information privacy, as do many of your colleagues.

Privacy is not dead. Yet the variety of ways in which corporations use and sell our most personal digital information has grown exponentially over the last decade. Loopholes in federal laws have allowed systemic, unfettered access to private, identifiable health records and Health and Human Services has been unable or unwilling to use any of its enforcement authority.² Medical records are sold and shared, typically without patient consent, knowledge, or advance notice. For example, many electronic health record (EHR) vendors obtain rights to own or sell all identifiable patient data as part of the contracts they require of physicians' offices and hospitals.³ Similarly, Change to Win, a federation of unions representing six million members, recently discovered that CVS Caremark's *iScribe* e-prescribing program obtains absolute rights to sell all identifiable data to drug manufacturers, clearinghouses, and data analysis companies via a service agreement.

¹ Report Card of the 106th Congress on Privacy, Senate, December 14, 2000

² Five years after the implementation of the HIPAA Privacy Rule, there still has not been one single civil penalty imposed even though there have been more than 40,000 complaints of privacy violations.

³ *Modern Healthcare*, "IT guru says some e-vendor contracts violate privacy" by Joseph Conn -- July 19, 2007

Efforts have been made by industry to distort the meaning of the word 'privacy' so that the ancient concept embodied by the Hippocratic Oath: that doctors protect their patients' secrets, has been turned upside down. Many in the industry seek to data mine the treasure trove of health information collected in every doctors' office for marketing, targeting, profiling and profit. In addition to the dramatic increase in the use of personal health data, it is far less secure than our electronic financial information and transactions. Since 2005, over 45 million health records have been breached and 250,000 Americans' health identities were stolen.

Ultimately, the consequences of disregarding privacy are far more severe than nosy neighbors or marketers learning about your medical procedure or diagnosis. When the wrong people see our health records, Americans can lose opportunities for jobs, insurance, credit and overall well being⁴. Even more tragic, when individuals are not confident that their health care will remain private, the fear of job loss, embarrassment and stigmatization can lead to suffering, delaying or even avoiding treatment, and ultimately even death. The California Health Care Foundation found that *one in eight* Americans has put their health at risk by engaging in privacy-protective behavior: Avoiding their regular doctor -- Asking a doctor to alter a diagnosis- Paying privately for a test - Avoiding tests altogether.

- According to HHS, **two million** Americans with mental illness do not seek treatment because of concerns about privacy.⁵
- **600,000** cancer victims do not seek early diagnosis and treatment.⁶
- **Millions** of young Americans suffering from sexually transmitted diseases do not seek diagnosis and treatment (1 in 4 teen girls are now infected with a STD).⁷
- The Rand Corporation found that **150,000 soldiers** suffering from Post-Traumatic Stress Disorder (PTSD) do not seek treatment because of privacy concerns.⁸

⁴ 35% of Fortune 500 companies admitted to looking at employee's health records before making hiring and promotion decisions (65 Fed. Reg. 82,467).

⁵ 65 Fed. Reg. at 82,779

⁶ 65 Fed. Reg. at 82,777

⁷ 65 Fed. Reg. at 82,778

⁸ "Invisible Wounds of War", The RAND Corp., p. 436 (2008)

RECOMMENDATIONS

Mr. Chairman, consumer trust is essential for acceptance of health IT and the willingness to participate in electronic systems. But trust is only attainable with privacy. We have a prime opportunity to move the health care system into the new century with the smart use of health information technology while safeguarding patient privacy. In fact, if we fail to restore privacy protections as we promote health technology, our hard work and billions of tax payer dollars will be wasted. We urge you to ensure the following measures of accountability, control and transparency are at the core of health IT legislation. Where applicable we cite specific provisions in the current Amendment in the Nature of a Substitute for the "Health Information Technology for Economic and Clinical Health Act" or the "HITECH Act".

1) ACCOUNTABILITY – Hold every entity with access to health information accountable. We have learned the painful lessons of letting industry set its own rules. Consumers no longer trust that corporations will use personal health information only as directed or guard it from theft or loss.

- Require those who collect, store or use personal health information to ensure that the data is accurate, reliable and secure.
- Require data encryption: we strongly support SEC. 4412 entitled Securing Individually Identifiable Health Information.
- Limit access to specific individuals via informed, electronic consent.
- Require audit trails of all electronic transactions, including treatment, payment and health care operations transactions as required in SEC. 4405 (c). We encourage you to require business associates to maintain audit trails as well as covered entities and to shorten the timeframe for this provision to go into effect.
- Authorize and fund Health & Human Services and the Federal Trade Commission to increase their oversight of industry practices including random audits of contracts. We strongly support SEC. 4411 requiring the Secretary to conduct periodic audits of covered entities and business associates.

- **Require breach notification:** the inclusion of SEC. 4402 is critical. However, we hope you will improve upon this provision by tightening the definition of a “breach”. The allowance of an “inadvertent” disclosure exception would appear to thwart the extensive sections contained within the HITECH Act to resolve data breaches of electronic medical records. Consequently, providing for an inadvertent disclosure does not seem to be in conformity with the broad intent of this provision. Under the current breach definition, all “inadvertent disclosures” would be excluded, and the bill’s enforcement and notice procedures would apply only to those breaches deemed to have occurred through criminal intent.
- **Ensure privacy safeguards and whistleblower protections, including meaningful enforcement of privacy rights.** The state attorneys general enforcement, a compensation scheme for privacy victims and applying penalties to business associates are essential provisions in the Improved Enforcement section (SEC. 4410).

2) CONTROL – Ensure individuals control the use of their personal health information.

Fundamental to the Code of Fair Information Practices and most professional Codes of Ethics is an individual’s right to control how their personal information is used.

- Codify a federal right to health information privacy.
- Ensure individuals can segment sensitive information and that safeguards for medical information are built in up front before problems arise. SEC. 3002(b)(2)(B)(i) requiring the HIT Policy Committee to make recommendations regarding segmentation is a positive step. We would encourage you to propose a stronger provision requiring the National Coordinator to ensure segmentation capabilities.
- Provide incentives for health IT systems to use electronic informed consent, innovative consumer privacy controls and for user interfaces to be accessible for patients with disabilities.

3) TRANSPARENCY – Protect consumers from abusive practices. Personal health information should not be sold and shared as a typical commodity. Health information is different; it is extremely sensitive and can directly impact jobs, credit, and insurance coverage.

Commercial transfers undermine routine privacy safeguards, including transparency and accountability.

- Prohibit direct or indirect remuneration for the sharing, disclosure or use of personal health information with limited exceptions for research and public health. **As stated previously, this protection for consumers provided for in SEC. 4405 (e) is essential.** As a privacy champion, you have an opportunity to put your mark on this provision with an important technical amendment. We urge you to strike the language "OBTAINED FROM ELECTRONIC HEALTH RECORDS" from the title of this provision. The current language could thwart the original intent of this provision because it suggests that the provision is only tied to EHRs, when we believe the drafters intended for this to apply both to electronic medical records and EHRs. Limiting the sale of information to PHI obtained from EHRs could exclude the primary activities this provision intended to prohibit, including:
 - Sale of identifiable prescription data
 - Sale of any information from a PHR
 - Sale of data by a business associate obtained from claims data or a non "EHR" source

Within this section, paragraph (1), we also recommend striking lines 8 – 15 beginning with the word "unless..." to remove the valid authorization clause. Societal ethics and mores led to a wise prohibition on the sale of blood or organs. Congress should similarly prohibit the sale of electronic medical records containing personally identifiable information. The release of private medical information can have far reaching consequences not only for the individual but for their children, grand children and other relatives.

Lastly, we would encourage a tightening of the language for the research and public health exception in SEC 4405 (e)(2)(A) by clarifying that only "not for profit" research fall into this exemption. Unless the word "research" is further qualified, the provision currently would allow any for profit company to sell records if they claim they are engaged in research. The inclusion of the phrase "public health" suggests that the

Written testimony of Patient Privacy Rights
Senate Judiciary Hearing: Health IT: Protecting Americans' Privacy in the Digital Age
January 25, 2009
Page 8 of 8

drafters intended to only allow a research exception to the prohibition on sale for not-for-profit research undertaken in the public interest. We urge the addition of the phrase "not-for-profit" to eliminate this inadvertently created loophole that appears to be inconsistent with the current language.

- Ensure that corporations cannot obtain exclusive or contractual rights to own or control personal health information.
- Personal health information obtained for one purpose must not be used for other purposes without informed consent. Even when consent is obtained, privacy obligations such as security and prevention of misuse, continue.

CONCLUSION

Americans are asking for accountability, control and transparency over how their personal information is used. We can do this. Making sure all of us trust the system and that consumers are protected is the key to success. Mr. Chairman, you have long led the fight to protect the right to be let alone. As you so passionately stated, "the right to privacy is a personal and fundamental right protected by the Constitution of the United States...It is important to come to grips with the erosion of our privacy rights before it becomes too late to get them back."⁹ **We could not agree with you more and ask that you continue to lead the way to protect our most sensitive information on earth.**

Sincerely,

Deborah C. Peel, MD
Founder & Chair

Ashley G. Katz, MSW
Executive Director
(512) 897-6390 (c)
(512) 732-0033 (o)
akatz@patientprivacyrights.org
www.patientprivacyrights.org

⁹ Report Card of the 106th Congress on Privacy, Senate, December 14, 2000

**Written Testimony of
Michael Stokes
Principal Program Manager, Microsoft Corporation's Health Solutions Group**

**Before the
Senate Judiciary Committee**

Hearing on Health IT: Protecting Americans' Privacy in the Digital Age

January 27, 2009

Chairman Leahy, Ranking Member Specter, and distinguished members of the Committee, my name is Michael Stokes, and I am a Principal Program Manager in Microsoft's Health Solutions Group. In this role, I focus on privacy issues, and I very much appreciate the opportunity to share Microsoft's views on the importance of privacy and health IT. We commend the Committee for holding this hearing today and for your efforts at the intersection of privacy, information technology, and healthcare reform. We are committed to working collaboratively with you, the Department of Health and Human Services, the Federal Trade Commission, consumer advocates, and other stakeholders to protect the privacy of health data.

Microsoft is here today because we are deeply engaged on both health IT and privacy issues. Over 12 years ago, Microsoft began developing technologies focused on the health industry, with the goal of using software and the Internet to transform healthcare, as they have so many other industries—opening new ways of working, new ways of communicating, and new economics. Our products, including HealthVault for consumers and Amalga for hospitals and health systems, are focused on driving scalable health IT solutions that can benefit all.

Microsoft also has a deep and long-standing commitment to privacy. We recognize that consumers will only be comfortable sharing their information if they trust that they will have control over its use and know that it will be protected. Establishing trust is especially important with respect to health data. This is because of the important role that health data plays in our overall healthcare system. Delivering quality, reliable healthcare requires that data be shared. New therapies, new cures, and new lessons about disease will be driven by the availability of health data. By working together to encourage data liquidity through strong privacy protections, we can realize the value of data sharing and thereby drive real change in our healthcare system.

Today, I want to discuss how we can promote the widespread use of innovative health IT solutions and the sharing of health data while still protecting privacy. My testimony today begins by describing what we believe to be the future of healthcare—a totally connected environment where patients and providers trust each other and use health IT to share information seamlessly. It then discusses how the three components of trust—transparency, control, and security—can provide flexible technology solutions that improve our current healthcare system. It concludes by showing how the same principles of transparency, control, and security underlie Microsoft's approach to privacy in health IT.

I. The Future: Dynamic, Trusted, Consumer-Driven Healthcare

There has been much discussion and debate about how to improve the healthcare system in the United States. But we think it is fair to say that we all have a single goal in mind: to deliver predictive,

preventive, and personalized medicine in an accessible, affordable, and accountable way. In our view, health IT and privacy are necessary elements to achieve this success.

A. Health IT Can Build a Patient-Centric System

The future of medicine and improvements in our healthcare system depend on the seamless exchange and reuse of health data. Today, in order to manage their health, consumers must deal with both paper documents and electronic files. Few people have the resources to keep track of medication lists, vaccination histories, appointment calendars, lab results, diet plans, exercise schedules, and all the other components of health data. Most people have little knowledge of how to prevent disease and little, if any, support for managing their healthcare.

What if consumers could collect all their health and wellness data electronically, could keep it securely stored in one place over time, and could share relevant elements of this record securely from provider to provider, no matter the doctor or insurance company with whom they interact? With all the relevant data at their fingertips, accessible at any time and any place, they could sign up for services that provide personalized alerts and information. They could track fitness goals across numerous devices, such as exercise bikes that monitor vital signs, smart watches that record the number of miles run, and scales that measure body fat as well as weight. They could research relevant medical conditions online and interact with support groups so that they would be better prepared and informed for their next visit to the doctor. And they could share data with their support systems and make better health decisions for themselves and their families.

A patient-centric system would benefit healthcare professionals and hospitals as well. Today, patients often see multiple doctors, often spread across multiple health systems. Each doctor sees only a fragment of the patient's health data, which can lead to unsound medical decisions and excessive costs. Health IT can connect an individual's existing data, allowing healthcare professionals to see a complete picture of their patient. This will enable providers to eliminate unnecessary procedures, avoid harmful drug interactions, and concentrate on providing better quality care.

At Microsoft, we believe technology can make this vision a reality without sacrificing privacy protections. We envision a healthcare ecosystem that places patients at the center of a protected and connected network, with:

- Patients as consumers—experiencing more control, more convenience, better service, and ultimately better value for what they spend on healthcare.
- Physicians as knowledge workers—professionals getting the right data in the right format at the right time to provide the best treatment and preventive care.
- New interactions among the key members of the healthcare ecosystem—physicians, patients, pharmacies, researchers, and insurance providers benefiting from a new flow of data to make better, faster decisions.
- The extension of modern healthcare to the virtual space—patients getting care when they want it, wherever they need it, thanks to virtual medical clinics, virtual doctor visits, virtual lab results, medical homes, and personalized medicine based upon genomic data.

- A learning healthcare system—one that measures key data points, identifies errors, and makes improvements in order to deliver value.

In this new healthcare system, everyone will have the right information at the right time with computer-assisted decision support, enabling the seamless exchange and reuse of data. Health data is the asset that will drive an efficient, high-quality, value-based, evidence-focused future for medicine, achieving one of the priorities of Congress and the new Administration.

B. Trust Is Essential to a Patient-Centric Healthcare System

Health data is the fuel that will drive a connected, patient-centric healthcare system. It is therefore critical that consumers, providers, and other participants in the healthcare ecosystem be willing to share health data. To facilitate such sharing, we must establish a foundation of trust.

Health data is often considered more sensitive than other personally identifiable information. If health data is stolen or lost, it is not simply a matter of recovering financial assets. It can impact an individual's employment, ability to receive healthcare, and social standing. And the effects are not limited to the individual whose data was lost, because health data may also be relevant to the person's children, grandchildren, or distant relatives. Indeed, there is evidence that many Americans do not actively participate in their own healthcare due to privacy concerns:

- According to the Department of Health and Human Services, two million Americans with mental illness do not seek treatment for this reason.¹
- Approximately 600,000 cancer victims do not seek early diagnosis and treatment.²
- Millions of young Americans suffering from sexually transmitted diseases do not seek diagnosis and treatment (1 in 4 teen girls are now infected with an STD).³
- The California HealthCare Foundation found that 1 in 8 Americans have put their health at risk by engaging in privacy-protective behavior: avoiding their regular doctor, asking a doctor to alter a diagnosis, paying privately for a test, or avoiding tests altogether.⁴
- The Rand Corporation estimated that 150,000 soldiers may be suffering from Post-Traumatic Stress Disorder (PTSD), many of whom do not seek treatment because of privacy concerns.⁵

¹ Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,779 (Dec. 28, 2000).

² *Id.* at 82,777.

³ *Id.* at 82,778; Press Release, Centers for Disease Control and Prevention, Nationally Representative CDC Study Finds 1 in 4 Teenage Girls Has a Sexually Transmitted Disease (Mar. 11, 2008), <http://www.cdc.gov/STDConference/2008/media/release-11march2008.htm>.

⁴ California HealthCare Foundation, *National Consumer Health Privacy Survey 2005* (Nov. 2005), <http://www.chcf.org/topics/view.cfm?itemID=115694>.

⁵ RAND Corp., *Invisible Wounds of War* 55, 104, 436 (2008), <http://www.rand.org/pubs/monographs/MG720/>.

Because health data can be highly sensitive, consumers and healthcare providers will only share such data if they trust that the privacy of health data will be protected. When such trust is established, data will flow freely, benefiting all participants. Consumers will receive better information about appropriate treatments, medications, nutrition, and exercise. Healthcare providers will receive more reliable health data and greater patient compliance, which in turn leads to better quality care and improved cost efficiencies both for treatment of individual patients and for public health purposes. In short, effective privacy protections are critical to the success of health IT and healthcare in general.

II. Trust Requires Transparency, Control, and Security

Transparency, control, and security are necessary to help ensure that consumers and healthcare providers trust, and are willing to participate in, the healthcare system.

A. Transparency Can Help Stakeholders Understand How Their Data Is Used

Transparency is significant because it provides consumers with an informed understanding of a company's data collection practices, of how their data might be used, and the privacy controls available to users. Without transparency, consumers are unable to evaluate a company's services, to compare the privacy practices of different entities to determine which products and services they should use, or to exercise the privacy controls that may be available to them. Transparency also helps ensure that when consumers are dealing with a company that has adopted responsible privacy practices, consumers do not needlessly worry about unfounded privacy concerns that might prevent them from taking advantage of new technologies.

Transparency is especially important with respect to healthcare data. If patients do not understand what data is being collected, who has access to the data, and what the data will be used for, they may decide not to provide the information at all—not even to their treating physicians. Without this data, doctors will not be able to make fully informed treatment recommendations, and overall consumer health could suffer.

Providers need transparency too. They need to understand how the health data they make available to patients and others may be used; they need to know whether such data may be disclosed to third parties; and they need to feel comfortable that health data will be protected.

Transparency is also essential to ensure accountability. Regulators, advocates, journalists, and others have an important role in helping to ensure that appropriate privacy practices are being followed. But they can only examine, evaluate, and compare practices across the industry if companies are transparent about the data they collect and how they use and protect it.

B. Control Can Help Stakeholders Manage Their Data Effectively

Transparency by itself is not enough. Stakeholders also need control over where their data is, who is looking at it, and for what purpose. For example, control allows patients to decide when and under what conditions they want to receive alert services or medical information that might be relevant to them. And if providers can control where health data is going, they will be better able to comply with applicable laws, regulations, and policies.

Control is particularly important when the consumer or provider needs a proxy to guide his or her choices. Patients often need to share data with custodians, guardians, or family members, but they may

want to ensure that the data is only shared under certain conditions (e.g., only when the patient is unable to make decisions for himself) or only for certain periods of time (e.g., only data about the past year rather than the patient's entire lifetime). Similarly, physicians often rely on nurses, staff, specialists, and laboratory technicians to provide care for a patient. Access controls can help ensure that the patient's health data is shared only with the healthcare professionals who need to see it, and that the patient's data is not inadvertently misplaced or deleted.

At the same time, however, control should not impede the flow of clinical data that healthcare professionals need to provide effective care. For example, some members of the healthcare community have pointed out that a system requiring repeated patient consents for the disclosure of clinical data could potentially hamper treatment in situations where care must be coordinated among multiple physicians. We all need to work together to create an environment that facilitates rather than hinders care.

C. Security Can Give Stakeholders the Confidence to Adopt Health IT Innovations

Concerns about the collection and use of personal data, widely publicized security and data breaches, and growing alarm about healthcare fraud and identity theft threaten to erode public confidence in digital health solutions. Cybercriminals are increasingly exploiting personal data to make a profit, and there are a growing number of security attacks that target personal data. A recent report from the Department of Health and Human Services noted that medical identity theft can lead to patients receiving the wrong care because of inaccurate data on their health records, being blocked from receiving health insurance or other benefits, or incurring financial obligations for services that were never provided.⁶

Security helps ensure that patients and providers do not spend time and resources dealing with data breaches, identity theft, and security flaws. Once stakeholders feel confident that their data is secure, they will be more willing to adopt the innovative health IT solutions that can improve care and reduce costs. Moreover, health IT can also improve security. For example, technology that verifies patients' identities, monitors access to health records, and identifies anomalies in services requested could help prevent and detect medical identity theft.⁷

D. Transparency, Control, and Security Provide Flexible Privacy Protections

Privacy protections are not just about patients. Doctors have data of their own that they want to keep private. Additionally, hospitals, insurance plans, research facilities, and other healthcare organizations are major businesses that need to protect their intellectual property and trade secrets. Transparency,

⁶ Booz Allen Hamilton & Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, *Medical Identity Theft Final Report* (2009), <http://www.hhs.gov/healthit/documents/MedIdTheftReport011509.pdf>.

⁷ *Id.* at 14 (noting, for example, that IT systems can "review transactional records and detect such anomalies as the appearance of treatments for chronic conditions not previously diagnosed; increases in prescriptions that may indicate drug-seeking behavior; or attempts to receive care at multiple locations, all remote from the individuals' residences").

control, and security protect privacy in ways that are flexible enough to accommodate all stakeholders in the healthcare system, not just consumers.

Moreover, today's healthcare ecosystem consists of a complex mixture of legacy and new, innovative solutions. Retrofitting existing systems may require significant design changes, and it may not be viable for everyone to upgrade their technology systems. One potential path forward is to provide a combination of simpler, less flexible, baseline solutions and newer, more complex, extensible technologies that encourage migration toward a more privacy-protective future. Following the principles of transparency, control, and security enables participants to provide privacy protections that are flexible and vibrant enough to support all of these technical solutions and business models.

III. Microsoft's Efforts to Build Trust Through Transparency, Control, and Security

Microsoft or anyone that provides tools and technologies involving healthcare data must adopt strong privacy practices that support trust. If people feel that the privacy of their healthcare data is not being protected, they will make less use of healthcare information technologies, which can hurt them and the healthcare industry alike.

Microsoft has been deeply engaged on privacy issues. Microsoft was one of the first companies to appoint a chief privacy officer, an action we took nearly a decade ago, and there are now several hundred employees throughout the company who focus on privacy as part of their jobs. We have a strong set of internal policies and standards that guide how we do business and how we design our products and services in a way that respects and helps protect user privacy. And we have made significant investments in privacy training and in building our privacy standards into our product development and other business processes.

A. Transparency by Providing Clear Disclosures

Microsoft is committed to providing transparency in its products and services. One example is HealthVault, Microsoft's free Internet-based platform that allows consumers to store copies of their health records, upload data from home health devices, share data with healthcare providers, and access products and services to help improve their health. HealthVault's privacy statement is designed to be easy to understand. We have eliminated passive language, and we wrote the statement at a high-school reading level. We also organized the privacy statement in terms of a consumer's perspective on how to use the HealthVault service, much like an abbreviated help document. We use third-party seals such as TRUSTe and eHon, we ask advocates and regulators to review our policy before launches and major revisions, and we encourage users to provide feedback.

Moreover, the HealthVault network currently has 40 live applications—programs that can connect with HealthVault, such as personal health records and alert services. Some of these applications are provided by Microsoft's partners. Before any application is authorized to access a consumer's data, we make sure that the consumer knows which application is requesting the data, what data is being requested, what the data will be used for, and which data elements are required or optional. HealthVault also stores audit trails, so that consumers can see who has accessed their health records and what actions have been taken.

B. Control by Offering Granular Access

Microsoft has made user control a key component of our healthcare solutions. We provide many different tools to help users control how their data is accessed and used. For example, in HealthVault, consumers can control what type of data is shared, who else has access to that data, whether others are allowed to modify or only to view the data, and how long others can access the data. These tools give consumers the flexibility to adjust their access decisions as their health needs change, so that a consumer who is suddenly diagnosed with a serious condition can immediately start sharing relevant data with his treating physician. Moreover, consumers can designate other "custodians" who can then share access with others, enabling records to be transferred from parent to child as the child reaches maturity or from elderly parent to adult children for extended care.

We have also implemented control features in our other health IT products. For example, just under a year ago, we launched Amalga, our family of enterprise data sharing and intelligence solutions, which connect a hospital's or health system's existing legacy systems and any new systems. This allows patient data to be viewed and queried holistically, enabling a shift from departmentally focused systems to more patient-centric systems. Amalga includes controls that allow hospitals and health systems to determine which data is shared when and with whom.

C. Security by Following Comprehensive Best Practices

Security has been fundamental at Microsoft for many years as part of our Trustworthy Computing initiative, and we have taken a broad approach to protecting the security of personal information. This approach includes implementing technological and procedural protections to help safeguard the information we maintain. For example, Microsoft has developed a Security Development Lifecycle program that calls for security evaluations and an appropriate combination of security measures, such as independent security penetration testing, independent certifications including ISO 27001, information segmentation, Lightweight Directory Access Protocol (LDAP) integration, auditing and logging capabilities, controlled-access facilities, and encrypted Internet protocols when communicating personal health data. We also have taken steps to educate customers about ways to protect themselves, and we have worked closely with industry and law enforcement around the world to identify security threats, share best practices, and improve our coordinated response to security issues.

IV. Conclusion

Microsoft recognizes that technology is only a part of a comprehensive approach needed to drive real change in our healthcare system. Education, leadership in healthcare organizations, and meaningful public policy are also critical components to success. We look forward to partnering with you and all participants in the healthcare ecosystem to move toward dynamic, trusted, and consumer-driven healthcare. Thank you for giving us the opportunity to testify today.

Advancing Health IT While Protecting Privacy: A Trust-Based Approach

The future: dynamic, trusted, consumer-driven healthcare. At Microsoft, we envision a healthcare ecosystem that places patients at the center of a protected and connected network, with everyone having the right information at the right time to make the best health decisions. Health data is the asset that drives the system, and health IT is the tool that enables the seamless exchange of health data.

Trust is essential to a patient-centric healthcare system. For the system to succeed, participants must be willing to share health data. Because health data can be highly sensitive, consumers and healthcare providers will only share data if they trust that their privacy will be protected. When trust is established and data flows freely, everyone benefits:

- Consumers receive better information about appropriate treatments, medications, nutrition, and exercise.
- Healthcare providers receive more reliable health data and greater patient compliance, which in turn leads to better quality care and improved cost efficiencies.

In short, effective privacy protections that establish trust are critical to the success of health IT and healthcare in general.

Trust requires transparency, control, and security. Transparency, control, and security are necessary components of trust.

- Transparency can help stakeholders understand how their data is used. If patients do not understand what data is being collected, who has access to the data, and what the data will be used for, they may decide not to provide the information at all—not even to their treating physicians. Providers need transparency too, so that they understand how the health data they make available to patients and others will be used, know whether such data will be disclosed to third parties, and feel comfortable that health data will be protected.
- Control can help stakeholders manage their data effectively. Control allows patients to decide when and under what conditions they want to share data with family members, receive alert services, or view relevant medical advertisements. If providers can control where health data is going, they will be better able to comply with applicable laws, regulations, and policies.
- Security can give stakeholders the confidence to adopt health IT innovations. Security helps ensure that patients and providers do not spend time and resources dealing with data breaches, identity theft, and security flaws. Once stakeholders feel confident that their data is secure, they will be more willing to adopt the innovative health IT solutions that can improve care and reduce costs.

Transparency, control, and security protect privacy in ways that are flexible enough to accommodate all stakeholders in the healthcare system, not just consumers. These principles are also sufficiently flexible to support today's complex mixture of legacy technical solutions and business models.

Microsoft is committed to offering trusted health IT solutions. The same principles of transparency, control, and security underlie Microsoft's approach to privacy in its health IT products, including HealthVault for consumers and Amalga for hospitals and health systems. Microsoft also recognizes that technology is only a part of a comprehensive approach needed—education, leadership in organizations, and meaningful public policy are other key components. We look forward to partnering with the public sector and all participants in the healthcare ecosystem to move toward a dynamic, trusted, and consumer-driven healthcare system.



January 21, 2009

Sen. Patrick Leahy
433 Russell Senate Office Building
Washington, DC 20510

Dear Senator Leahy:

Thank you for inviting Vermont Information Technology Leaders, Inc., to submit written testimony to the Senate Judiciary Committee on the issue of privacy and security in the electronic exchange of protected health information. We appreciate your interest in this subject area, which is critical for achieving President Obama's goal of having electronic medical records in widespread use by 2014, and for building the National Health Information Network to exchange data between various parts of the health care delivery system.

Vermont Information Technology Leaders, Inc. (VITL) is a non-profit public-private partnership that has been designated by the Vermont General Assembly as the exclusive operator of the statewide health information exchange network. VITL receives funding from both federal and state sources to help physicians acquire and effectively use electronic health records systems, and to connect those EHR systems to the statewide network. VITL's network will eventually be connected to systems operated by regional health information organizations in adjoining states and the national network.

Since VITL's incorporation in July 2005, we have made significant progress. We ran a successful pilot project which involved making medication claims data from health plans available to the emergency departments at two Vermont hospitals so that clinicians have a list of the prescription drugs a patient has taken in the last year. The service is still in operation and has been expanded to a third hospital emergency department. VITL has been working with the Vermont Department of Health to build a chronic care information system so that clinicians can better manage conditions such as diabetes and hypertension.

We have built all the core components of the statewide network infrastructure and have developed a Clinical Transformation Program, which helps physician practices change their workflows and clinical processes to make full use of EHR systems. Several independent primary care practices are now using EHR systems funded by VITL's grants. We are ready to connect those practices, and others who financed their own EHR systems, to VITL's network so that they can begin exchanging data. VITL is planning to launch an advanced health information exchange pilot project in at least one Vermont community during 2009, with rollout to other areas of the state following shortly thereafter.

1

VITL gained valuable experience from its medication history pilot in the areas of patient consent and developing business associate agreements with requirements for protecting the privacy and security of health information. More than 90 percent of patients arriving in emergency departments of participating hospitals are "opting in," or giving permission for clinicians to access their electronic medication histories. Since the service began operating in April 2007, there have been no problems reported with maintaining privacy and security.

Vermont's privacy laws are more stringent than the privacy rules contained in HIPAA. VITL's legal counsel has advised us that Vermont's patient privilege statute requires that patients affirmatively give permission, or opt in, before their protected health information can be accessed. Compliance with this and other state laws, as well as applicable federal rules and laws, has been foremost on our minds as we have sought to find acceptable policy positions. The task has been made somewhat more complicated by the fact that many Vermonters seek health care at academic medical centers outside the state's borders, including those in Lebanon, N.H., Albany, N.Y., and Boston, Mass. Looking ahead to the day when clinicians providing care at those facilities are able to access the Vermont health information exchange to gather information on their Vermont patients, we realized that the policies developed for the Vermont exchange must be in alignment with the privacy laws in those other states.

VITL has been working on privacy issues since 2006, when we joined the Health Information and Security Privacy Collaboration (HISPC). The Vermont Health Information Technology Plan published in July 2007 contains a chapter on privacy and security. VITL intensified its work in this area in March 2008 when it began the task of developing privacy and security operational policies for the statewide health information exchange network. These policies will govern the exchange's day-to-day activities, including data access, patient consent, auditing and monitoring, security requirements, and procedures for handling a breach and notifying those affected.

We understood early in the policy development process that it is very important to have input from both consumers and health care providers, so we scheduled a series of six face-to-face meetings that were held monthly from April 2008 to September 2008. Participants in those discussions included advocates for civil rights and patients' rights, the elderly, people with mental health issues, and people with disabilities. Several health care provider organizations were represented, including the state's largest provider of mental health services. The Vermont Agency of Human Services, the Vermont Department of Health, the Vermont Health Care Ombudsman's Office, and the Vermont Department of Banking, Insurance, Securities, and Health Care Administration all sent representatives.

Over the course of those meetings, and from feedback gathered by circulating meeting summaries to other interested parties, several general themes became apparent.

Consumer representatives desire that:

- 1) Consumers have the ability to control who accesses their information, and determine what information they are able to see. Advocates said some consumers fear that their care could be unfavorably biased if clinicians are able to access mental health notes and other sensitive information.
- 2) Health information exchange participants are required to meet stringent security measures, and there is tough enforcement of policies, with sanctions for violations.
- 3) Consumers are notified immediately of any privacy or security breaches, even if they did not result in protected health information being compromised or inappropriately accessed.

Health care provider representatives recommend that:

- 1) Consumers should not be able to restrict their access to health information, as physicians and other clinicians need to know as much as possible about their patients in order to provide effective and high

quality care. If consumers are able to block access to pieces of data, clinically relevant information may be missing, they said.

- 2) Participation in the health information exchange should not place more administrative work on already overburdened physician practices and hospitals.
- 3) VITL not act as a "policeman" on security issues, but instead should only provide guidance to exchange participants on adequate security measures.

It is important to note there wasn't unanimity with the above positions from within the ranks of the constituencies. For example, some individual providers told us they don't have a problem with consumers being able to restrict access to information on the health information exchange. Likewise, in a telephone survey of 500 adult Vermonters conducted by VITL in April 2007, 19 percent of the consumers surveyed said they believe health care providers should have full access to patient health information, even if it means providers having access to information that some patients may want to keep private.

A key finding from the April 2007 consumer telephone survey was that 67 percent of the Vermonters polled said they believe there needs to be a balance between patient privacy and the degree to which health care providers have access to health information about their patients.

With consumer advocates and health care provider organizations representing different positions along the patient-privacy continuum, VITL's staff and consultants attempted to draft policies that struck a balance. A subgroup of VITL's Board of Directors began reviewing the draft policies in November 2008, and was in the midst of the process when the Office for Civil Rights in the Department of Health and Human Services published new guidance as part of DHHS's "Privacy and Security Toolkit to implement The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information." Members of the VITL board's privacy and security subgroup found the guidance to be informative, and compiled an analysis of the six principles laid out by the OCR, as well as applicable federal and state laws. The analysis was used during discussions of VITL's draft policies and will be included in the forthcoming update to the Vermont Health Information Technology Plan.

As of this writing, members of the VITL board's subgroup are waiting to learn which privacy and security requirements will be included in the economic stimulus legislation, before finalizing the Vermont operational policies. But based on the work they have done so far, here are VITL's recommendations:

- **Congress should mandate that patients must opt-in before data is made available via an electronic health information exchange.** This type of patient consent would be consistent with the Individual Choice Principle outlined by the Office for Civil Rights in its recent guidance. It would also provide more uniformity between states.
- **Patients should have the right to receive educational information, as well as a Notice of Privacy Practices, before being asked for consent.** This provision would help the patient make an informed decision.
- **The Health Information Technology Standards Panel (HITSP) should be instructed to expedite development of more advanced technical standards for protecting patient privacy.** A Basic Patient Privacy Consent standard exists that supports patient opt-in, but it does not support more sophisticated controls.

- **Congress should revisit the issue of granularity (consumers being able to determine access to data) when adequate technical standards are in place.** When advanced patient privacy consent standards are widely supported by vendors, additional privacy protections could be considered.
- **Consumers should have the right to receive an audit log from the health information exchange showing when their data was accessed and who accessed it on the exchange.** This would be consistent with OCR's Openness and Transparency Principle.
- **Health information exchanges should be required to send a notice periodically to patients who have opted in.** This notice would remind patients that their health data is being exchanged and that they have the right to opt-out at any time. To reduce costs, electronic notification should be permitted.
- **A national standard definition of security breaches should be adopted, as well as requirements for notification of those affected.** This would reduce confusion and provide uniformity.
- **The Office of the National Coordinator (ONC) should regularly publish recommended security measures for health information exchange that are scalable to organization size.** This would help providers keep up to date and establish more consistent practices from user to user.
- **The use of protected health information should be prohibited for marketing or other commercial purposes not directly related to treatment, payment, or health care operations, unless the patient has specifically authorized use.** De-identified data from a health information exchange should be available for research, quality improvement, and public health purposes.

If you or your staff have any questions about the above recommendations, we would be glad to answer them and provide additional information. We thank you for the opportunity to provide input into this important legislative process, and we look forward to additional federal support for health IT so that we may accelerate our efforts to improve the quality and effectiveness of health care that Vermonters receive.

Sincerely,



Gregory Farnum
President