AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

DISCUSSION DRAFT OF HEALTH INFORMATION TECHNOLOGY AND PRIVACY LEGISLATION

HEARING

BEFORE THE

SUBCOMMITTEE ON HEALTH

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

JUNE 4, 2008

Serial No. 110–122

Printed for the use of the Committee on Energy and Commerce

energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE

55–462 PDF WASHINGTON : 2008

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 ENERGY AND COMMERCE

JOHN D. DINGELL, Michigan, *Chairman*

HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
Vice Chair
LOIS CAPPS, California
MIKE DOYLE, Pennsylvania
JANE HARMAN, California
TOM ALLEN, Maine
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
DARLENE HOOLEY, Oregon
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
CHARLIE MELANCON, Louisiana
JOHN BARROW, Georgia
BARON P. HILL, Indiana

JOE BARTON, Texas
Ranking Member
RALPH M. HALL, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee

PROFESSIONAL STAFF

DENNIS B. FITZGIBBONS, *Chief of Staff*
GREGG A. ROTHSCHILD, *Chief Counsel*
SHARON E. DAVIS, *Chief Clerk*
DAVID CAVICKE, *Minority Staff Director*

SUBCOMMITTEE ON HEALTH

FRANK PALLONE, JR., New Jersey, *Chairman*

HENRY A. WAXMAN, California
EDOLPHUS TOWNS, New York
BART GORDON, Tennessee
ANNA G. ESHOO, California
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
Vice Chairman
TOM ALLEN, Maine
TAMMY BALDWIN, Wisconsin
ELIOT L. ENGEL, New York
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
MIKE ROSS, Arkansas
DARLENE HOOLEY, Oregon
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
JOHN D. DINGELL, Michigan *(ex officio)*

NATHAN DEAL, Georgia,
Ranking Member
RALPH M. HALL, Texas
BARBARA CUBIN, Wyoming
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
STEVE BUYER, Indiana
JOSEPH R. PITTS, Pennsylvania
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
JOE BARTON, Texas *(ex officio)*

CONTENTS

	Page
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, opening statement	1
Hon. Nathan Deal, a Representative in Congress from the State of Georgia, opening statement	3
Hon. Henry A. Waxman, a Representative in Congress from the State of California, opening statement	4
Hon. John D. Dingell, a Representative in Congress from the State of Michigan, opening statement	5
Hon. Marsha Blackburn, a Representative in Congress from the State of Tennessee, opening statement	6
Hon. Anna G. Eshoo, a Representative in Congress from the State of California, opening statement	7
Hon. Michael C. Burgess, a Representative in Congress from the State of Texas, opening statement	9
Hon. Gene Green, a Representative in Congress from the State of Texas, opening statement	10
Hon. Joe Barton, a Representative in Congress from the State of Texas, opening statement	11
Hon. Lois Capps, a Representative in Congress from the State of California, opening statement	12
Hon. Tim Murphy, a Representative in Congress from the Commonwealth of Pennsylvania, opening statement	13
Hon. Tammy Baldwin, a Representative in Congress from the State of Wisconsin, opening statement	14
Hon. Hilda L. Solis, a Representative in Congress from the State of California, opening statement	15
Hon. Edolphus Towns, a Representative in Congress from the State of New York, opening statement	16
Hon. Bart Gordon, a Representative in Congress from the State of Tennessee, opening statement	17
Hon. Diana DeGette, a Representative in Congress from the State of Colorado, prepared statement	174

WITNESSES

Steven J. Stack, M.D., Member, Board of Trustees; Chairman, HIT Advisory Group, American Medical Association	18
Prepared statement	20
Byron Thames, M.D., Member, AARP Board of Directors	31
Prepared statement	33
Frances Dare, Director, Cisco Internet Business Solutions Group	41
Prepared statement	43
Marc C. Reed, Executive Vice President, Corporate Human Resources, Verizon Communications Group, Inc.	53
Prepared statement	55
James A. Ferguson, Executive Director, Health IT Strategy & Policy, Kaiser Permanente	63
Prepared statement	65
Joycelyn Elders, M.D., Former U.S. Surgeon General, Co-Chair, African American Health Alliance	76
Prepared statement	78
Deborah C. Peel, M.D., Founder and Chair, Patient Privacy Rights	86
Prepared statement	88
Deven McGraw, Director, Health Privacy Project, Center for Democracy and Technology	95

Page

Deven McGraw, Director, Health Privacy Project, Center for Democracy and Technology—Continued
Prepared statement 97
Carolyn M. Clancy, M.D., Director, Agency for Healthcare Research and Quality, Department of Health and Human Services; accompanied by Susan D. McAndrew, J.D., Deputy Director for Health Information Privacy, Office for Civil Rights, Department of Health and Human Services 150
Prepared statement 153

SUBMITTED MATERIAL

Divided We Fail, letter of June 2, 2008, to Messrs. Dingell, Barton, Pallone, and Deal 176
eHealth Initiative, statement of Janet M. Marchibroda, dated June 4, 2008 178
Consumer Partnership for e-Health, letter of June 3, 2008, to Messrs. Dingell, Barton, Pallone, and Deal 188
Healthcare Leadership Council for the Confidentiality Coalition, letter of June 4, 2008, to Messrs. Dingell, Barton, Pallone, and Deal 191
Oregon Institute of Technology, statement submitted by Michael Kirshner, D.D.S., M.P.H., dated June 4, 2008 197
Federal Trade Commission, letter of June 3, 2008, to Mr. Dingell 201

DISCUSSION DRAFT OF HEALTH INFORMATION TECHNOLOGY AND PRIVACY LEGISLATION

WEDNESDAY, JUNE 4, 2008

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON HEALTH,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:07 a.m., in room 2123, Rayburn House Office Building, Hon. Frank Pallone, Jr. (chairman of the subcommittee) presiding.

Present: Representatives Pallone, Waxman, Gordon, Towns, Eshoo, Green, DeGette, Capps, Baldwin, Schakowsky, Solis, Matheson, Dingell (ex officio), Deal, Pitts, Rogers, Myrick, Murphy, Burgess, Blackburn, and Barton (ex officio).

Also Present: Representative Gonzalez.

Staff Present: Bridgett Taylor, Purvee Kempf, Yvette Fontenot, Jason Powell, Bobby Clark, Hasan Sarsour, Lauren Bloomberg, Alex Haurek, Ryan Long, Melissa Bartlett, and Chad Grant.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. PALLONE. The meeting of the subcommittee is called to order. And today we are having a hearing on the Health Information Technology and Privacy discussion draft. And I have now recognized myself for an opening statement.

Our Nation's health care system is arguably one of the most inefficient and costly systems in the industrialized world. We spend approximately $2.7 trillion, or $7,600 per person, annually on health care, approximately 16 percent of our Nation's gross domestic product. But what has this money bought us? Studies show that in spite of all our spending, we do not fair any better on important health measures than countries that spend a lot less. Skyrocketing health care costs, inconsistent quality, and huge disparities in access are just a few of the problems that we face.

Health care experts around the country agree that health information technology could improve our system by making it safer and less costly. In this modern age, I find it unbelievable that our health care system is so out of date. Thanks to modern technology, a person can manage their finances from their home PC, or order a pizza with a click of the button, and yet most patients and providers rely on antiquated systems that are counterproductive to the

delivery of health care. Patients are prompted to recall their entire medical history everytime they see a medical provider. A lapse in memory could lead to duplication of services or worse, medical errors. And pharmacists struggle to make sense of handwritten prescriptions. Emergency rooms are forced to treat unconscious patients without knowing their complete medical history and no way to ascertain that information. And all of these problems could be solved, I believe, with HIT.

In addition, we would achieve enormous savings from the widespread adoption of HIT. The potential savings is estimated to be anywhere from $81 billion to $170 billion annually. Such savings would occur by improving coordination of care, patient safety, as well as disease management and prevention efforts. At a time when the cost of health insurance and medical services continue to skyrocket, we could use those savings to help improve access for some of the 47 million uninsured Americans.

While some providers have already begun to make the investment in HIT, far more have not, essentially because of serious financial and operational barriers. I don't know if he has arrived yet, but one of the freeholders in New Jersey, Jim Carroll of Bergen County, was supposed to be here today. And I use him as an example of someone who is trying to take the initiative to modernize the medical facilities in his area of my State. And he has shown me firsthand the challenges that these communities face, but that is why the Federal Government should take a more proactive role at facilitating the adoption of a nationwide interoperable HIT infrastructure.

The draft legislation we are reviewing today seems to accomplish that goal. The discussion draft before us would codify the Office of the National Coordinator for Health Information Technology, which would have key responsibilities, such as designing a strategic plan for the development and implementation of a nationwide HIT infrastructure. The draft also would establish two Federal advisory committees that would advise the National Coordinator by making recommendations on policies and technical standards.

In order to promote the electronic exchange and use of information, the discussion draft also directs Federal agencies to use HIT that meet adopted standards, which would help move the private sector toward the adoption of HIT as well.

And the draft also includes financial incentives for providers to adopt and use HIT through three new grant programs. The first program will offer competitive grants for providers to purchase HIT with a preference for small health care providers, providers in medically underserved areas, and others that have difficulty in acquiring HIT on their own.

The second program is for States and tribes that will help leverage private sector dollars in order to provide low interest loans to help providers purchase HIT.

And finally, the third program provides support for local or regional organizations to develop HIT plans.

This draft also takes an important step towards protecting patient privacy. The draft would close a number of loopholes under the existing regulatory framework that governs patient privacy and security. It would also provide patients with more options to control

their health information and require patients be notified when their protected health information has been breached. And I know that the issue of patient privacy is very important to members on both sides of aisle, including myself. While I think the provisions included in the discussion draft would do a lot to improve the protection of patient privacy, I recognize there may be various views on this, and I am looking forward to hearing some of those views today and working with my colleagues as we move forward with this draft.

I said at the beginning of my statement we need to move forward with modernizing our Nation's health care system, and investing in HIT today will help make our system more efficient tomorrow, thereby lowering costs and saving more lives.

I just want to thank some of my colleagues who have worked so diligently on the development of this draft, particularly Chairman Dingell, who this has been a top priority, as well as Ranking Members Barton and Deal. I am pleased that we have been able to work with our Republican colleagues and make this a bipartisan effort.

I also want to recognize the efforts of Congressman Waxman, Congressmen Markey, Towns, Gordon, Eshoo, Capps, and Gonzalez, all of whom have been instrumental in the development of this draft. Again, it is a draft and we are continuing to seek input on a bipartisan basis relative to the interoperability, the privacy sections, as well as the funding mechanisms.

So I now recognize Mr. Deal for 5 minutes.

OPENING STATEMENT OF HON. NATHAN DEAL, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF GEORGIA

Mr. DEAL. Thank you, Mr. Chairman. I want to thank you for holding this hearing today in order to evaluate legislation which will promote the adoption of information technology in the health care system. In my mind, the expansion of health HIT is one of the most fundamental reforms that we should make to improve health care delivery. The creation of an electronic system to track medical records will sharply reduce the number of medical errors and help eliminate inefficiencies and waste in the system.

Health HIT systems hold the potential to significantly improve health care by eliminating illegible handwritten prescriptions, providing immediate access to laboratory test results, and making a patient's full medical history available to their treating physician no matter where that patient seeks treatment.

I appreciate the Chairman's willingness to produce a bipartisan proposal on this issue, and I look forward to continuing to work with him and with our subcommittee chairman as we move forward in developing a bill for introduction. It is my hope that the legislation will strike an important balance so that the congressional action does not impede or limit reforms which are already transforming this marketplace.

Innovators, health care providers, health care payment systems, and patients should drive the changes. We are already seeing many hospitals, physicians, pharmacies, and payors moving forward in the implementation of this technology. However, I believe we can speed the adoption of these technologies through targeted congressional action.

I have been pleased by Secretary Leavitt's leadership in promoting many discussions and demonstrations on health HIT, which will be helpful in its future. I believe the proposal we are considering today will help ensure this momentum will not be lost when we have a change of administration next year.

There remain some issues which I hope we can continue to explore through this hearing. Our proposal makes some changes to existing medical privacy laws to ensure that patients' personal medical records remain private as health care moves into the electronic realm. I look forward to our witnesses' feedback on this issue as we seek to balance these protections while maintaining a workable framework so that patients can reap the benefits of better health care through the use of technology.

The draft does not contain any stark or anti-kickback relief allowing providers to receive health information hardware and software without triggering the penalties of that statute. This issue was a major component of our work on health IT last Congress, and I hope our witnesses can speak to the appropriateness of its inclusion in what we do this year.

In conclusion, I want to thank the witnesses on both panels for their participation in this hearing today and hopefully we can all move forward to produce a meaningful piece of legislation. I yield back my time.

Mr. PALLONE. Thank you, Mr. Deal.

Mr. Waxman.

OPENING STATEMENT OF HON. HENRY A. WAXMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. WAXMAN. Mr. Chairman, I want to thank you for holding this hearing to examine the complex issues surrounding the promotion of electronic health information technology. I think the draft that we have been provided is an improvement, and I thank you for the hard work you and your staff put into it. The use of electronic health information has many potential benefits, including promoting swift and effective communication between multiple health care providers that may be coordinating the treatment of a patient; however, as we continue to develop and use health information technology, we must ensure that sufficient privacy and security protections are in place.

Our health care system will not be effective if privacy fears deter Americans from seeking appropriate treatment. Unfortunately, survey after survey demonstrates that American consumers lack confidence that their privacy and security of their personal health information will be protected. Moving health records into electronic form is only likely to increase this anxiety.

We have also had continuing reports of privacy and security breaches. This has served as a warning about the need for attention to this issue.

According to Privacy Rights Clearinghouse, over 200 million records containing sensitive personal information of U.S. residents have been compromised because of security breaches since 2005. The Administration's lax approach to enforcing existing medical privacy requirements has raised additional concerns. A recent L.A.

Times article reported that the Administration has not imposed a single civil fine under the Federal Medical Privacy Rule, despite over 30,000 complaints of violations since the rule has been in effect. And I am pleased that the discussion draft contains a number of important privacy protection and security protections, including provisions to require breach notification, to encourage entities that maintain health information to share the least amount of data necessary with other entities, and to extend privacy requirements to certain entities that handle health information but are not currently covered by the Federal health privacy rule.

I believe this draft represents an improvement. I think it is important we consider whether other steps should be taken to ensure appropriate protections for consumers, such as additional tools to promote improved enforcement of Federal health privacy law, and in this regard I am very interested in learning what the views are of our distinguished panelists regarding these and other provisions.

I also want to underscore that the process of developing standards for health information technology systems should ensure public input from all the diverse stakeholders and government should play the leadership role in this area. Today's hearing is an important step towards that end.

Mr. PALLONE. Thank you, Mr. Waxman. The gentleman from Pennsylvania, Mr. Pitts.

Mr. PITTS. Thank you, Mr. Chairman, for scheduling this very important hearing on a very important issue. I look forward to hearing our distinguished witnesses, and I will reserve my time.

Mr. PALLONE. Mr. Dingell, the Chairman of the Full Committee, recognized for an opening statement.

OPENING STATEMENT OF HON. JOHN D. DINGELL, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. DINGELL. Mr. Chairman, thank you for your courtesy. I commend you for this hearing. It is a very important matter. The hearing today will focus on a legislative discussion draft, and I want to emphasize that so that our comments may be properly focused. And we hope that this draft will lead us to a discussion and to the enactment of legislation that will improve the quality and efficacy of health care in this country through the adoption of a good new Health Information Technology, HIT.

We have before us an opportunity to increase our Nation's ability to provide better quality of care, significantly reduce health care costs, and to strengthen the privacy protections of the American people in a new electronic world.

The care provided by doctors, nurses, pharmacists, and other health care entities is based on information about the individual patient, such as medical history, previous treatments, past surgeries, drug allergies, and much more. If that patient's information is inaccurate or incomplete, it can lead to devastating consequences such as serious medical errors or the failure to detect dangerous conditions early on. Furthermore, giving health care providers access to a patient's up-to-date medical history could reduce costs by avoiding unnecessary or duplicative diagnostic testing or treatment.

The discussion draft legislation that we will focus on today represents a strong bipartisan agreement of the need to facilitate the creation of health information systems that are electronically maintained and exchanged. It codifies the Office of the National Health Coordinator for Health Information Technology in order to develop and implement a nationwide HIT infrastructure, which includes use of electronic health records for all individuals as well as electronic exchange of health information amongst those entities that are essential for the delivery of health care.

An additional but fundamental component of this legislation will strengthen the law to ensure that the privacy and security of an individual's health information are well protected, a matter of major concern. The discussion draft fills in the gaps in the current law to ensure that an individual's electronic personal health information is only used for legitimate and appropriate purposes.

I want to thank the witnesses who will be testifying today on this legislation. I want to thank my colleagues on both sides of the aisle for encouraging the establishment of a more effective health care system in this country.

I am particularly proud of the work done by our good friend and colleague, the Ranking Minority Member, Mr. Barton, by Subcommittee Chairman Pallone and Ranking Member Deal in developing this new draft bill. I also want to acknowledge the important contributions and the leadership of Ms. Eshoo, Mr. Rogers, Mr. Gordon, Mr. Waxman, Mr. Gonzalez, Mr. Markey, Mrs. Capps, and Mr. Towns. All of them have made enormous contributions to moving these matters forward, and I want to thank them and congratulate them. I look forward to working in a bipartisan manner on this legislation so that we may introduce and then move forward with this important legislation to address major concerns of the country with regard to better, cheaper, and more efficiently delivered health care.

Thank you, Mr. Chairman.

Mr. PALLONE. Thank you, Chairman Dingell. The gentleman woman from Tennessee, Mrs. Blackburn, recognized for an opening statement.

OPENING STATEMENT OF HON. MARSHA BLACKBURN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE

Mrs. BLACKBURN. I want to thank you, Mr. Chairman, for the hearing to discuss the draft legislation. And I want to welcome everyone who is here to talk with us and work with us through this process. I do believe that it is critical for Congress to focus on transforming our health care system because there are three things that we really can do with this: we can improve quality; we can reduce costs; and we can facilitate better access for all Americans through the implementation of health IT. Congress will connect patients, doctors, hospitals, and the entire extended health care community to provide realtime data sharing between all sectors of the health system.

In my district in Tennessee, Hurricane Katrina was a stunning reminder of the vulnerability of our health care system as individuals from the Gulf Coast came to the Memphis area to seek med-

ical care. Quite simply, the storm exposed the weaknesses of the Nation's health IT infrastructure.

We can transform the American health system from an outdated model based on paper records stored in filing cabinets—how outdated does that sound—to a comprehensive and secure electronic system that is accessible by patients, physicians, health care providers in any circumstances and on an as-needed basis. How wonderful that would be.

The benefits of health HIT are just not theoretical. From our Department of Health and Human Services, they are reporting that medical records can reduce health spending as much as 30 percent annually. There are 98,000 deaths each year caused by medical errors. This could be reduced if health care providers had access to complete information and treatment histories for their patients.

Tennessee is actually a leader in this arena. The State of Tennessee implemented the E-health initiative, which provides all of our routine care patients with an electronic record. That is our Medicaid delivery system in Tennessee. The State estimates for every dollar spent on the new technology they are saving between $3 and $4 in duplicate tests and medical errors.

In addition, Tennessee is one of nine States participating in a project to coordinate multiple local health information connections through the CMS Office of the National Coordinator for Health IT. We also have Vanderbilt University Center, which has implemented a highly functional, interconnected computerized health IT system. They have lowered their costs dramatically by streamlining their records keeping and improving patient care.

We are looking forward to hearing from each of you and looking forward to what we can save in dollars, but also how we can improve the quality of life for all of our citizens and how we can improve the delivery of health care for all Americans. And I yield back.

Mr. PALLONE. Thank you. Next is the gentlewoman from California, Ms. Eshoo, who has been a leader on this issue for a long time. I recognize her for an opening statement.

OPENING STATEMENT OF HON. ANNA G. ESHOO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Ms. ESHOO. Good morning, Mr. Chairman. And thank you. Welcome to all of the witnesses. Thank you for being here. Especially Ms. Dare, who hails from Texas but whose company, Cisco Systems, is part of the region that I have the privilege to represent: Silicon Valley. It is one of the leading, obviously, technology companies in the world.

In February of this year, I had the privilege of hosting a health care forum at Stanford University with President John Hennessy; Dr. Zerhouni, who heads up the NIH; Speaker Pelosi; and other top experts from the medical and health care community. Our discussion really centered in and around a vast reshaping of our health care system. It didn't deal with the issues that we take up here incrementally, and that is the gaps in health insurance for children, those that are uninsured. It is not what our discussion was about. And front and center there was unanimity amongst all of the par-

ticipants that fundamental changes have to occur in our health care system to incorporate and to leverage the benefits of technology.

It was said by, I believe, other members of the Committee that we live in the Information Age, but health care, one of the most information intensive segments of our economy, remains mired mostly in a paper-and-pen past. We can buy airline tickets from a home computer, we can pay our taxes online, we can even buy a car with a few mouse clicks, but our health care system remains dangerously disconnected. Patients' medical histories are largely disaggregated amongst the various physicians who treat them, and they are often inaccessible to a new doctor or even to the patients themselves.

So we have a lot of work to do. We recognize it. It is how we are going to do it. And these inefficiencies cost. They cost the patient, they cost the system, they cost the taxpayer. It really doesn't speak very well about a country that leads in technology that we would have one of the major economic sectors of our economy that is left mired in this pen-and-paper past.

To accelerate the adoption of HIT and create market conditions incentives, which it is going to take that. It is not just going to take the legislation. The legislation has to bring in the stakeholders because they are going to have to be making investments and we have to encourage the investments that have to be made across the country.

Representative Mike Rogers, a member of this committee, and myself introduced H.R. 3800 last October. It is called the Promotion of Health Information Technology Act. It is bipartisan legislation, obviously, and it is endorsed by a very diverse group of organizations, the AARP, the Business Roundtable, SCIU, the Information Technology Industry Council, the American Electronics Association, and the Health Care Information and Management Systems Society.

Our bill builds on the excellent work that Senators Kennedy and Enzi have done, which has also garnered broad support in the Senate and which is likely to secure Senate passage in the coming weeks. My hope was that the committee would take that bill up because it is bicameral, bipartisan, it has industry, employer, patient and professional support. But we have a draft discussion before us today and Chairman Dingell chose to go the direction that we are going, and I look forward to working with everyone because I have a real commitment to this.

The discussion draft closely resembles H.R. 3800 in almost all respects and includes the important principles that it sets forth. I think that any meaningful HIT legislation must establish a process for the rapid formulation and implementation of standards to facilitate the exchange of interoperable health data and create incentives to ensure that the technologies are actually adopted.

Like H.R. 3800, the draft bill established a streamlined process for the adoption of HIT and requires the government to abide by the standards it sets. If we do the legislation well, there will be a lot of power to it and that power of HIT stands to transform the American health care system. I think that that is really clear. But

without the aggressive action by the Congress to promote and adopt it, we won't see the benefits of these innovative technologies.

We have to keep in mind that the Federal Government is——

Mr. PALLONE. The gentlewoman is 2 minutes over.

Ms. ESHOO. I will conclude.

The most significant player in health care in the Nation. So the standards that we set are the standards that will be the model for the rest of the country.

So, Mr. Chairman, I look forward to this, and I thank the witnesses again.

Mr. PALLONE. Thank you. The gentleman from Texas, Mr. Burgess.

OPENING STATEMENT OF HON. MICHAEL C. BURGESS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. BURGESS. Thank you, Mr. Chairman. I also want to thank you for holding the hearing today. It looks like we have got a great panel ahead of us. I think it is important that we always hear from our medical community, but I am anxious to also hear from the technology companies and from the patients to help inform our Federal information technology policy.

So this bill that we have in front of us, I have been studying it. I hope I can hear from the panel today how this will be helpful. I am not entirely convinced myself, but I do know that any time this committee sits down and works on legislation pertaining to the practice of medicine, I always get a little nervous because unintended consequences—remember, unintended consequences used to take a generation to come back and bite us. Now they seem to be doing it in about 4 months. So unintended consequences are something that I really want to concentrate on in this legislative hearing.

I was greatly concerned that this draft would have required any new electronic transaction to require patient consent. It is important that we protect the privacy of sensitive patient information, but we shouldn't do the one thing that would kill digitizing medicine, complicating the normal and routine in medical treatment by requirements with which patients would have a difficult time in complying.

We heard the Chairman talk about codifying the Office of the National Coordinator on Health Information, that it could be a positive step. I wait to hear the testimony of the panel in front of us today. Five years ago when I arrived here, this was talked about as something that was going to bring great change to the information technology community and medicine and 5 years later it hasn't happened, and yet the private sector has moved forward with several initiatives that I think are extremely compelling, and I do hope we get to visit about those today. The standards, the interoperability. My understanding is there are private companies out there now who are dealing with this and dealing with it quite successfully. So I wonder why we need to codify that into Federal law. But maybe I am wrong. And I will certainly be willing to listen to that testimony.

I am uncertain whether providing the financial incentives such as grants will be effective. We have great testimony from Dr. Stack

and I certainly look forward to hearing his information, but I would be remiss if I did not mention the one thing that he brings out in his testimony, this 10 percent reduction in physician reimbursement rates that we built into the structure that is happening in less than 4 weeks time. It is critical that we address that. I urge my colleagues to look at 6129, that would temporarily halt those cuts for 7 months fully paid for by the same offset we used in the Medicaid moratorium. So I certainly appreciate the AMA being here this morning and bringing that issue to our attention.

This committee does not have jurisdiction over antitrust-related issues and we have to address that in order to further use and encourage the deployment of health information technology. I believe the administration's rule in providing an exception to the physician's self-referral prohibition at a safe harbor under the anti-kickback statute are certainly short of the mark as far as the underlying changes we need to make in the Starr clause to fully integrate our solo or group medical practices and integrate those with the emergency room at the hospital. Allowing for the donation of equipment or an electronic health record is a good first step, but the law still prohibits closer contractual agreements between doctors' offices, hospitals and other health care providers.

I have introduced other legislation, 5885, the Health Information Technology Promotion Act of 2008, that would accomplish just that. I think we need to tackle this artificial legal separation in order to do what many of the advocates say they want to do and bring medicine into the digital economy.

Thank you, Mr. Chairman. I will yield back.

Mr. PALLONE. Thank you. I recognize our vice chair, Mr. Green, for an opening.

OPENING STATEMENT OF HON. GENE GREEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. GREEN. Thank you, Mr. Chairman, for holding the hearing on the discussion draft of the health information technology and privacy legislation. There is no question that widespread use of electronic health records and the need for prescribing will bring tremendous benefits to the health care sector and the patients it serves. We know that health IT is a potential for health care savings and for coordinating care.

For a number of years, I have introduced a bill called the Generic Assessment and Chronic Care Coordination Act. This lack of coordinated care in our country is startling. But if we could coordinate our care through health IT, we would have the potential to change our health care system. We have always seen electronic health records and need for prescribing as a goal, but have been less certain on how to reach that goal. However, I think that the perfect example for the need for health IT is what happened during Hurricane Katrina. In Houston, we welcomed more than 150,000 residents from New Orleans and Louisiana. And the only example we had of being able to treat those folks was the electronic records system that was developed within the VA and the medical professionals at Houston VA Medical Center were able to access the health records for the evacuees who had typically received care at the VA hospital.

I stood out at the Astrodome and watched people getting triaged because they didn't bring their medicine, they didn't remember what type of medicine they brought. But with the veterans, we were able to get their care very quickly. So with this information in hand, there is no doubt that our VA doctors were able to provide the evacuees with better care.

We need to determine the best approach to create a comprehensive system that operates effectively and yields significant benefits for both patients and providers. We also need to ensure that our systems are interoperable so that we can actually achieve our goal of coordinating care in our move to facilitate the implementation of health IT. Let us make sure that the privacy laws have been enacted to protect our patients.

Make no mistake that today's paper records should be behind us and it is a matter of efficiency and quality care. We have overwhelming support on both sides of the aisle for the development of the health information technology, and I am pleased the committee draft worked in a bipartisan manner to come up with this. And I look forward to hearing from our witnesses.

And with that, Mr. Chairman, again thank you for the hearing. I welcome our witnesses and yield back my time.

Mr. PALLONE. Thank you, Mr. Green. Next I recognize for an opening statement the ranking member of the full committee, Mr. Barton.

OPENING STATEMENT OF HON. JOE BARTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. BARTON. Thank you, Mr. Chairman. Today we are reviewing a bipartisan discussion draft that has been developed with our stakeholders in the staffs of both the Republican and the Democrat members of this subcommittee and full committee. The draft before us today is largely based on what we have heard from the health IT community. They believe and it is most of us on this subcommittee believe something must be done to accelerate the widespread adoption of health IT.

The discussion draft that we have today reflects the need to push forward to establish the public/private partnership with the government and the market to develop and implement a truly interoperable health care system so that every person in this country will have an electronic medical record by 2014. I applaud this goal. I applaud this product. I believe that health IT holds the promise of actually providing some real savings in overall health care spending as well as improving health outcomes for patients.

The discussion draft before us today reflects the need to look at how health information currently moves through the vast health care system to provide providers and plans and their business associates and identifies a few gaps where the current HIPAA regime could be strengthened. I will name just a few.

First, the draft promotes better enforcement against parties that cause the harm. Today if a business associate is the party that improperly used or disclosed the participant's information, there is no HIPAA enforcement by the government against the business associate. This gap is filled in by the discussion draft.

The draft also provides patients with the right to know when a breach of their information has occurred. There is currently no breach notification requirement in HIPAA. This gap is also filled in in the discussion draft.

Mr. Chairman, let me express my gratitude to you and to full committee Chairman Dingell for the opportunity to work in a bipartisan basis. I think this draft shows that when we do really work in a bipartisan basis, we can work together through the committee to build legislation that will work. I would ask our colleagues on both sides of the aisle to continue to work on this product to fine-tune it at the subcommittee and full committee level so we can move a bill through committee and on to the floor and hopefully on to the other body and pass a bill that the President can sign this year.

I yield back the balance of my time.

Mr. PALLONE. Thank you. The gentlewoman from California, Mrs. Capps.

OPENING STATEMENT OF HON. LOIS CAPPS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mrs. CAPPS. Thank you, Chairman Pallone. And I appreciate the fact that we are having this hearing today and for your and Chairman Dingell's tireless work to get a bill moving on HIT and privacy. And I appreciate the array of witnesses, expert witnesses, that we have here for this hearing. The issue that is before us has been percolating for years and it is a credit to you both, Chairman Dingell and Pallone, that we are moving forward today.

Health care is probably one of the last few industries that is dominated by a paper-based recordkeeping system. As a nurse, I know all too well what it is like to try to maintain a bulging cabinet—several cabinets filled with medical files. I also know what it is like to try to read through a large file containing years of information often haphazardly organized and perhaps with some important pieces having slipped away.

It is quite frustrating that while I can be confident in J. Crew having a record of what color and sized pants I ordered in 2002, my physician may not know the last time I had a tetanus shot.

A national standard for implementation of electronic health record systems is long overdue, and I am very supportive of Titles I and II of the draft bill that address adoption and testing.

It is my hope that today we can discuss some issues of great importance. Countless breaches of personal health information have occurred over the last several years as electronic records have become more common. First and foremost, we lack a clear definition of privacy and the right to privacy and security with respect to personal health information. I believe defining this right is key to ensuring greater protection for our patients.

Furthermore, we need to specify language regarding the segregation of sensitive health information which was recommended by the National Committee on Vital Health Statistics.

Other areas of improvement I would like to see are public lists where security breaches have occurred and a more explicit mandate of security measures like encryption and audit trails.

I do want to thank the Committee for putting together this draft. It is a great way to start this conversation and for seriously considering the important privacy issues that need to be addressed. Expanding the scope of which entities are covered is crucial.

So Mr. Chairman, I thank you for all of your attention to these issues, and I do look forward to continuing to work with you and with all of us on them. And thank you and I yield back.

Mr. PALLONE. Thank you, Mrs. Capps. The gentleman from Pennsylvania, Mr. Murphy, recognized for an opening statement.

OPENING STATEMENT OF HON. TIM MURPHY, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF PENNSYLVANIA

Mr. MURPHY. Thank you, Mr. Chairman. I am happy to see this bill being considered by committee. A couple of years ago, my friend Patrick Kennedy and I had introduced legislation dealing with health information technology and seeing that at that time as an important cost savings and patient quality and patient saving measure. We have a $2 trillion health care system in this country and some $400 to $500 billion of that each year is wasted, wasted on unnecessary tests of avoidable complications and several other elements where you see the system not working as well.

All of us have experienced in our families sometime when someone got an X-ray, you showed up at the doctor's office and he said do you have that X-ray with you. No is your response, I didn't carry this large package with me. That is OK, he will say, we will just order another and another and another and another. And those costs add up. And it is the death by those thousand cuts that is crippling the cost of our health care system. By adopting electronic medical records, we can reduce health care costs perhaps as much as 30 percent. RAND Corporation said $162 billion in direct savings and perhaps another $150 billion a year in otherwise lost work time and lost wages and lost productivity. We can save massive amounts.

We also have to understand just in terms of what this means for patient frustration and those darn clipboards we have to fill out on every floor of every hospital that don't get to the next department to make it on. Like my colleague across the aisle, I too, when I have worked at hospital, would oftentimes be seeing patients, and as pediatric patients may only be a few weeks old or a few years old and yet there would be voluminous files and somehow in a few minutes we would have to go through those and find important information, information that if we had at our finger tips could make a huge difference in cost savings and an improved diagnosis and care of the patients.

I hope we get to a point in this Nation when it is seen as commonplace and people will feel comfortable with carrying a credit-card sized medical record in their wallet that they are assured is private and secure and safe. I want to know that myself or family members if they are ever in an accident or unconscious, someone can access that easily and readily but with proper security and proper confidentiality.

It seems to me in this Nation if we figured out a way to prevent nuclear missiles from launching, we ought to be able to figure out

a way to keep patient records safe and private in whatever mechanisms are possible. But what we have to see here is a way of using this aggressively to lower health care costs by improving patient safety and patient quality.

I am delighted to be here and look forward to either hearing or reading about the testimony today. We have some people that have some great experience on what has been done. I am looking forward to that. And, Mr. Chairman, I think this is a vitally important bill to move forward and move forward on this. It literally will help us save lives. I yield back.

Mr. PALLONE. Thank you, Mr. Murphy. The gentlewoman from Wisconsin, Ms. Baldwin.

OPENING STATEMENT OF HON. TAMMY BALDWIN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WISCONSIN

Ms. BALDWIN. Thank you, Mr. Chairman. I appreciate the fact that you are holding this important hearing today. I am really happy that we are taking time today to focus on health care IT. Like many of the other members who have spoken before me, I wanted to add my voice of support. I would also like to commend Chairman Dingell, Chairman Pallone, Ranking Member Barton, and Ranking Member Deal for working together to create the health care IT discussion draft that we will be reviewing and examining today. Congressional action on this topic I think is long overdue, and I am hopeful that we can continue to work in a bipartisan spirit and take some first steps on supporting and encouraging health care IT adoption.

It is easy to understand why health care IT is so popular. The potential for error reduction, reduction of duplicative tests and exams, the decision support that is provided with many of the health care IT packages, it has such potential for improving patient care, making better use of scarce resources, and frankly the collection of data for research potential is huge. Imagine the opportunities for medical collaboration with health care IT that it can provide a rural doctor who needs to consult with a specialist who is hundreds and maybe even thousands of miles away, or imagine the research potential that this deidentified or anonymized electronic data holds to learn and understand things like dangerous side effects of a widely prescribed drug as just one example.

So I am encouraged that we are taking up this important topic. I am glad to see that the discussion draft codifies the Office of the National Coordinator for Health Information Technology. This is a basic and first step that is long overdue. I am also glad that the discussion draft provides some much needed resources for providers to adopt health care information technology into their practices: The financial barrier to health care IT adoption is very significant and these resources will help ensure that all Americans have access to health care IT systems as a part of the health care they receive.

So again, Mr. Chairman, thank you for holding this hearing and thank you to the witnesses who are about to testify.

Mr. PALLONE. Thank you. The gentlewoman from California, Ms. Solis, recognized for an opening.

OPENING STATEMENT OF HON. HILDA L. SOLIS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Ms. SOLIS. Thank you, Mr. Chairman. I also want to commend you for convening this hearing today. As the development and implementation of health information technology moves forward, I would like to just bring up the notion that we do not leave communities of color and underrepresented communities behind. Latinos, Asians, African-Americans and Native Americans face a wide range of health care disparities, including lack of access to health insurance and lack of diverse health professionals, and bear a disproportionate burden of impact of chronic and preventable diseases.

According to the National Association of Community Health Centers, only 8 percent of health centers are using electronic health record systems compared to 18 percent of private office-based primary care physicians. I am proud that the South Central Family Health Center in Los Angeles has taken the lead in planning health IT activities for the Community Clinic Association of Los Angeles County. They recently received a grant from the Health Services and Resource Administration to help plan for adoption of electronic health records and other IT innovations.

This is a good step in the right direction, yet many of the individuals that I represent in Los Angeles County represent low-income families who are under-insured and uninsured and depend on community health clinics and a safety net hospital system to provide and receive their care. Many of these health care providers, especially community migrant and homeless health centers, do not have the ability to adopt health IT.

I am pleased at least today that the discussion draft before us will help provide funds for health IT for such organizations. I believe that HIT holds promise as a tool to reduce health care disparities by ensuring that language assistance is also present to facilitate effective communication between health care professionals and their patients with limited English proficiency. In L.A. County alone, nearly one out of three residents, or approximately 2.5 million people, speak a language other than English at home. However, health IT standards must take into consideration persons with limited English proficiencies. This is why I will be asking the GAO to examine health IT standards and language access and believe we must ensure that underrepresented communities and those who provide care to them are part of the process and solution.

I look forward to hearing from our witnesses. I just want to make one last note, that the Health and Human Services Office of Civil Rights has a tremendous workload now. And I believe that business associates should also be accountable for violations of the HIPAA privacy rule. The Office of Civil Rights, as you know, is already overburdened by existing privacy complaints, and consequently complaints related to discrimination, language access and racial and ethnic health disparities are not being adequately addressed in my opinion. And I hope that we can find ways to make sure that the Office of Civil Rights will have adequate resources and personnel to conduct these additional duties.

So I thank the witnesses today and I thank the chairman for having this hearing.

Mr. PALLONE. Thank you, Ms. Solis. And next for an opening statement, the gentleman from New York, Mr. Towns.

OPENING STATEMENT OF HON. EDOLPHUS TOWNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

Mr. TOWNS. Mr. Chairman, I would like to waive my opening statement and basically to thank you and, of course, Dingell and, of course, Deal and everybody who put together this working document. And I think that it is important that we move forward with this because when we look at disparities and all of that I think that this provides us an opportunity to correct a lot of things that are going on. And let me just make this statement and then I am going to close, that when it comes to health and health record, it is amazing what is going on out in the world. You know, a whole hospital closed and, of course, the records were just thrown in the street and—I mean, that to me is just unbelievable in this day and age.

So I think that when we look at the health IT, I think that maybe we will be able to empower people that need to be empowered when it comes to their health and the health care. So, Mr. Chairman, thank you very much and I yield back.

Mr. PALLONE. Thank you, Mr. Towns. I think that concludes our opening statements by members of the subcommittee. So we will now turn to our witnesses. And I see the panel is seated in front of us. I want to welcome all of you here today. And let me introduce the members of the panel. I will start from my left to right.

First is Dr. Steven Stack, who is a Member of the Board of Trustees and Chairman of the HIT Advisory Group for the American Medical Association. Then is Dr. Byron Thames or Thames, AARP Board of Directors from here in D.C. And then we have Ms. Frances Dare, who is Director of Cisco Internet Business Solutions Group from Richardson, Texas. And Mr. Marc Reed, who is Executive Vice President of Corporate Human Resources for Verizon Corporation. And then we have Mr. James Ferguson, who is Executive Director, Health IT Strategy and Policy for Kaiser Permanente. And welcome next is Dr. Joycelyn Elders, who is the former U.S. Surgeon General. Thank you for joining us today. And she is also Co-Chair of the African American Health Alliance out of Little Rock, Arkansas. And then we have Dr. Deborah Peel, who is Founder and Chair of the Patient Privacy Rights Organization in Austin, Texas. And finally Ms. Deven McGraw, who is Director of the Health Privacy Project for the Center for Democracy and Technology here in Washington, D.C.

And he is not speaking today, but I did want to mention since he came in—I mentioned him in my opening statement—is freeholder Jim Carroll from Bergen County, New Jersey, who as I mentioned before has taken the initiative in trying to spread health IT throughout our medical centers in the northern part of New Jersey. Thank you for being here today as well.

The way we operate I think you know is that we essentially hear 5-minute opening statements from each of you. Try to limit it to

that if you can because we have a big panel. Your statements become part of the hearing record. And we may at the discretion of the subcommittee submit additional brief and pertinent statements in writing, questions essentially for you to follow up on later. And I will now recognize Dr. Stack to begin.

Dr. STACK. Thank you.

Mr. GORDON. Mr. Pallone, I am sorry. I was in a markup. But could we ask by unanimous consent that I be able to give a brief opening statement or is that too out of order?

Mr. PALLONE. No, it is not out of order. Without objection, so ordered. And Dr. Stack will let Mr. Gordon make an opening statement.

Mr. GORDON. I want to say nice things about you, but I need to find it.

Mr. PALLONE. You don't have to say nice things about me, Bart.

OPENING STATEMENT OF HON. BART GORDON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE

Mr. GORDON. OK. Again, thank you, Mr. Chairman, for allowing me to have this opportunity. And I want to make very clear that I fully support Chairman Pallone and Chairman Dingell's efforts to have Congress play a more active role in developing a national electronic health care record infrastructure. The goal of this draft legislation is to promote and improve current Federal efforts. HHS is behind schedule and little progress has been made since the President's announcement in 2004. In addition, HHS has yet to develop a strategic plan on how it intends to proceed.

If we want to develop a seamless network of electronic health care information, key components are the technical standards to ensure interoperability, security, and electronic authenticity for confidentiality. However, technical assistance alone is not enough, there must be also be technical conformance tests and test beds to guarantee software products meet the required standards.

When the financial services, banking, retail, and manufacturing and telecom industries faced similar challenges in developing these technical standards and conformance tests, they turned to a single Federal agency for assistance, the National Institute of Standards and Technology, or NIST. Working with these industries in the private sector, NIST developed standards and tests that have been beneficial for NIST efforts. Last year, the Committee on Science and Technology reported out a bipartisan bill to use NIST in addressing these technical issues. Through resolution of technical hurdles, it is necessary first—the first step toward broadly developing health care IT, it is important that Congress takes a comprehensive approach to addressing this issue.

I believe this bill we are discussing today does that. The draft legislation highlights the importance of technical standards and conformance tests and acknowledges NIST's experienced and proven track record.

I want to thank Chairman Pallone and Chairman Dingell for working with me in addressing this key issue. Most of the focus of EHR has been as cost saving measures. As we recall, a CBO report stresses EHRs have the potential to significantly reduce costs. However, our focus should also be on the demonstrative fact that

a fully operable EHR system can improve patient care and make it easier for our health care professionals to do their job. Health care costs are important. However, the bottom line is we should make every effort to improve the quality and efficiency of care delivered to our constituents.

Once again, I want to thank you, Chairman Pallone, and Chairman Dingell and your staff for working with us and putting it together, as well as the minority. This has been a good collaborative effort and we are going to get a good bill and a good product. Thank you.

Mr. PALLONE. Thank you. Would the gentlewoman from North Carolina like to make an opening statement?

Mrs. MYRICK. No. I will waive.

Mr. PALLONE. OK. Thank you. We will go back to our panel and start with Dr. Stack. Thanks.

STATEMENT OF STEVEN J. STACK, M.D., MEMBER, BOARD OF TRUSTEES, CHAIRMAN, HIT ADVISORY GROUP, AMERICAN MEDICAL ASSOCIATION

Dr. STACK. Good morning. My name is Steven Stack, and I am a practicing emergency physician and Chairman of the Department of Emergency Medicine at St. Joseph Hospital East in Lexington, Kentucky. I also serve as a trustee on the Board of the American Medical Association. Thank you for the opportunity to testify on health information technology and some of the ways we can make these advances work for patients and physicians.

The AMA commends the subcommittee for both its work to accelerate the transition to an interoperable nationwide HIT infrastructure and for highlighting the important role of the Federal Government in advancing the technological transformation of the health care industry. When properly implemented in a connected environment, widespread HIT adoption has the potential for transforming the practice of medicine by putting critical clinical information in the hands of physicians at the point of care.

As an emergency physician serving the patients of central Kentucky, I can't emphasize enough how essential it is to have rapid access to complete and accurate appellant information in the fast-paced, information-poor environment of the emergency department.

In my clinical practice, a robust nationwide HIT system would be an invaluable tool in the provision of high quality, at times life altering care for those in need of urgent treatment. Recognizing the potential benefits of HIT, many physicians are already considering the incorporation of HIT in their practices. But we realize that we still have a long way to go. To aid this process, constructive solutions to several persistent challenges will make HIT not only desirable, but also a viable and embraced patient care tool. It is in the creation of these solutions that we believe that the government has an important facilitating role to play along with the broader health care community.

To that end, we commend you for your proposed roadmap that clarifies the role of the Office of the National Coordinator for HIT as a driver and strategic planning for the development, adoption, and use of HIT. Efforts such as this will help in the creation of a

robust HIT network that efficiently and reliably moves data smoothly among health care providers.

Additionally, the AMA agrees that the establishment of advisory committees comprised of expert stakeholders who would develop and recommend the technical standards, connectivity, implementation, and interoperable specifications and certification criteria is needed. And with their central role in the successful implementation and clinically use of those advanced systems, we strongly recommend greater physician representation and involvement in this process.

As we work to create an interoperable nationwide HIT network, AMA would also like to thank the committee for working to strengthen the HIPAA privacy rule. Holding all parties with access to patient health information directly accountable for compliance with privacy standards is critical. In an electronic era where sensitive information can be made public with the touch of a button, constant vigilance to privacy concerns is imperative to preserve the rights and trust of our patients. This vigilance, however, should not become a barrier to the advancement of HIT, which offers great potential to improve the quality, safety, and efficiency of patient care.

Physicians are eager to embrace HIT. I would be remiss, though, if I don't remind us all that physicians are operating with progressively thinner or negative revenue margins. So financial incentives really are a critical factor in impacting the adoption rate. In fact, a full two-thirds of physicians say they will be forced to defer HIT and other technology purchases if this year's Medicare payment cuts occur as planned on July 1st. While some large health systems and hospitals have the necessary financial and human resources to adopt electronic medical records, many small physician practices, small business America, simply can't. It is truly essential, therefore, that financial incentives be made available and easily accessible, particularly to smaller physician practices which face the greatest technological, operational, and financial challenges.

I sincerely appreciate this opportunity to share our thoughts on your proposal for accelerating our Nation's move to an interoperable nationwide HIT infrastructure. We at the American Medical Association are actively working with physicians and other health care stakeholders to accelerate the adoption and realize the significant benefits of HIT. We thank you for the work of your committee, and we look forward to continued collaboration with you for the benefit of our patients.

[The prepared statement of Dr. Stack follows:]

Statement

of the

American Medical Association

to the

Committee on Energy and Commerce
Subcommittee on Health
U.S. House of Representatives

Re: Discussion Draft of Health Information Technology and Privacy Legislation

June 4, 2008

Division of Legislative Counsel
202 789-7425

Statement

of the

American Medical Association

to the

Committee on Energy and Commerce
Subcommittee on Health

U.S. House of Representatives

RE: "Discussion Draft of Health Information Technology and Privacy Legislation"

June 4, 2008

Thank you Chairman Pallone, Ranking Member Deal, and Members of the Subcommittee on Health for inviting me to provide comments on three primary elements being considered as part of the Committee's draft legislation on health information technology (HIT) and privacy. On behalf of our physician and medical student members, the American Medical Association (AMA) appreciates the opportunity to submit our statement on HIT. We hope our comments provide you with further guidance on legislative mechanisms needed to incentivize the rapid adoption of HIT. We commend the Subcommittee for recognizing the importance of moving toward an interoperable, nationwide HIT infrastructure and the crucial role the federal government plays in assisting the health care industry to accelerate the adoption and implementation of HIT systems and tools. When implemented properly in a connected environment, widespread HIT adoption will transform the practice of medicine and provide physicians with a powerful tool by putting real-time, clinically relevant patient information and up-to-date clinical decision

support tools in practitioners' hands at the point of care. Physicians agree that HIT is a means to improve patient safety, advance care coordination, and increase administrative efficiency. In order to achieve this reality, a coherent HIT environment will need to be highly connected, secure, affordable, and be integrated into the typical workflow of medical practices as diverse as those in large hospitals, community health centers, and among rural solo practitioners.

The AMA urges policymakers to give careful consideration to several points. HIT systems must operate in a robust network, which enables data to flow smoothly among health professionals and the differing HIT systems they rely upon. At present, the lack of connectivity among HIT systems presents a serious barrier to the effectiveness of HIT to significantly improve health care delivery. In addition, privacy and security of patients' confidential medical information should be of paramount concern. In an era when a patient's private, sensitive health care information can be made public with the touch of a button, it is imperative that strong privacy and security standards and protections be in place and be enforced against all parties that exchange, use, disclose, store, or otherwise handle patient health information. All sectors of the health care industry will benefit from physician HIT adoption, including the federal government, private payers, and consumers. Thus, any legislative proposal intended to promote widespread HIT must provide financial incentives that address true direct and indirect costs of adoption. Accordingly, the AMA urges Congress to provide direct financial assistance for physicians to adopt HIT, especially since physicians continue to face shrinking payer revenues that have failed to keep pace with the costs of their practices. We appreciate your consideration of our

comments and welcome the opportunity to work closely with you to promote HIT during this important and pivotal time for our health care delivery system.

A Connected HIT Environment

Perhaps the largest impediment to the effectiveness of HIT is the lack of connectivity of health care data among health care providers. Currently, most health care data, whether on paper or electronic, are trapped in "silos." As a result, a patient may have a physician or health system that uses HIT, but if that patient requires care elsewhere, the information from that system may not be accessible. A report from the Institute of Medicine has noted that "health information exchange," the anytime, anywhere access to clinical care information across traditional business boundaries, is essential for improving health care quality. HIT is simply a tool that enables users to more effectively store and manage data. However, without the necessary data, the value of HIT is significantly constrained. Therefore, the real benefits of HIT will only be realized in a highly networked environment in which data is liberated from those silos and shared appropriately with health care providers.

According to a February 2008 Government Accountability Office (GAO) Report, the U.S. Department of Health and Human Services (HHS) has not yet developed a national strategy that defines plans, milestones, and performance measures for reaching the President's goal of interoperable electronic health records by 2014. The GAO recommends that HHS establish detailed plans and milestones for the development of a national HIT strategy and take steps to ensure that its plans are followed and that milestones are met. A national strategic plan for developing HIT policies, standards,

implementation and interoperability specifications for an interoperable nationwide HIT infrastructure, which sets milestones and performance measures is needed. Currently, there are multiple government initiatives involved with HIT, including the Certification Commission for Healthcare Information Technology (CCHIT), the Healthcare Information Technology Standards Panel (HITSP), the National Institute of Standards and Technology (NIST), and the federal advisory committee known as the American Health Information Community (AHIC) and its future successor (AHIC 2.0). It is essential that this myriad of federal initiatives be coordinated to avoid conflicts and the duplication of efforts and that each agency focuses on areas of its greatest expertise and technical capability. Moreover, appropriate input from expert stakeholders into the development of interoperable, technical standards, implementation specifications, and certification criteria for health information exchange is critical. Expert stakeholders must be involved throughout the standard development process, including physicians who will use and are expected to invest most heavily in these advanced systems. Current government initiatives and advisory committees should incorporate greater physician representation and involvement, especially representation from small medical practices.

Privacy and Security of Patient Health Information

The AMA urges policymakers to make privacy and security of patient medical information a top priority. Privacy and security of patient information is a principle that physicians take very seriously. Information disclosed to a physician during the course of the patient-physician relationship is confidential to the greatest possible degree. Respect for patient

privacy is a fundamental expression of patient autonomy and is a prerequisite to building the trust that is at the core of the patient-physician relationship.

Physicians and others in the health care industry have devoted substantial resources and staff time to retooling their privacy policies and daily work flow practices to comport with the demands of the Health Insurance Portability and Accountability Act of 1996 Privacy Rule (HIPAA). Physicians would be reluctant to revisit this issue again so soon without assurances that the highest possible privacy and security protections are implemented without impeding their office practices. The AMA cautions against restricting or imposing additional requirements on physicians for the use and disclosure of health information that is currently authorized under HIPAA for treatment, payment, and health care operations purposes. These current permitted uses and disclosures are critical for ensuring that patients' access to care is not impeded or delayed.

Currently, the HIPAA Privacy Rule applies only to health plans, health care clearinghouses, and health care providers—so-called "covered entities." Yet, there are other parties that work with confidential health care records that are not required to comply with privacy rules. Examples of parties that may receive and use information and who are not covered by HIPAA include workers compensation carriers, researchers, life insurance issuers, employers, marketing firms, HIT and personal health record (PHR) vendors, and health information exchanges (HIEs). Many of the parties that covered entities contract with to perform administrative, legal, accounting, and similar services on their behalf, and that would obtain health information in order to perform their duties (called "business associates"), are beyond the law's authority to directly regulate or sanction. These gaps in

federal privacy protection coverage leave large volumes of identifiable health information vulnerable to improper access and disclosure without meaningful enforcement mechanisms or remedies. Forming a national health information infrastructure without adequate federal privacy protections threatens not only the privacy of patients, but also the viability of such a system. Patients cannot be placed in the untenable situation of being forced to withhold sensitive information essential to their diagnosis and treatment out of fear it may be improperly disclosed. Patients must believe in the security of their records for any HIT system to work. As we continue to move toward the electronic exchange of health information, it is crucial that protecting the privacy of health information remain a central element. Federal law also should ensure that those who improperly obtain, use, or disclose health information are subject to civil and criminal penalties. Therefore, we appreciate your efforts to expand the HIPAA Rules to directly cover additional parties involved in the electronic exchange, storage, use, or handling of health information that are not currently covered by the HIPAA Privacy and Security Rules.

Financial Incentives to Spur HIT Adoption

While physicians are optimistic about the promise that HIT holds to transform patient care through better access to patient records and improved office efficiencies, the adoption rate among physicians still remains relatively low. Approximately 20 percent of physicians in practices employing 21 or more physicians have some form of HIT, while adoption rates among smaller practices with 5 or fewer physicians range from 12 to 13 percent. Significant adoption barriers remain—these include lack of financial incentives, training, and technical support. In fact, there may be significant first-mover disadvantages because

early adopters are likely to pay the initial costs without receiving the benefits that will accrue only when a truly networked HIT system exists. The Congressional Budget Office (CBO) reported last month that HIT will not produce the extraordinary savings originally claimed by many including widely-cited reports that estimated that the use of HIT would result in $80 billion in net savings annually. CBO further stated that such reports "appear to significantly overstate the savings for the healthcare system as a whole—and by extension, for the federal budget—that would accrue from legislative proposals to bring about widespread adoption of health IT."

Although lack of interoperability and cost savings, discussed above, are barriers to physician adoption as they significantly reduce the clinical and business case for physician HIT investment, direct and indirect HIT costs are also an impediment, particularly for physicians practicing in small office settings. A study by Robert H. Miller and others found that initial EMR costs were approximately $44,000 per full-time equivalent (FTE) provider per year, and ongoing costs were about $8,500 per FTE provider per year. (*Health Affairs*, September/October, 2005). Initial costs for 12 of the 14 solo or small practices surveyed ranged from $37,056 to $63,600 per FTE provider. These costs are difficult to absorb for the over 50 percent of physician practices in this country that have 5 or fewer physicians, and account for 80 percent of outpatient visits, especially as these practices struggle to implement existing HIPAA requirements, Medicare and other public and private payer mandates while facing shrinking public and private payer revenues. Direct financial incentives are especially critical for small physician and rural practices that face the greatest financial, technological, and operational challenges.

A 2007 AMA survey showed that with a 10 percent Medicare physician payment cut in 2008, two-thirds of physicians will defer investments in their practice, including the purchase of new medical equipment and information technology. If rates are cut by 40 percent by 2016, about 8 in 10 physicians will forgo these investments. For the majority of physicians dealing with multiple financial issues, ranging from low reimbursement under Medicare and Medicaid, declining revenue from managed care, professional liability insurance premiums, and the cost of complying with state and federal mandates, investing in HIT systems is challenging.

A variety of technical and workflow issues pose additional cost barriers to more widespread adoption of HIT. Implementing HIT in a clinical setting is much more complicated than connecting a computer to the Internet or installing software from a CD-ROM. Systems must conform to the workflow of a practice or the workflow must be modified so that the HIT system does not impede it. Physician offices, particularly small practices and those in rural or underserved areas, need simple and inexpensive solutions to obtain the benefits of HIT. Physicians will need time and money to effectively transform the workflow of their practices. The AMA strongly believes that meaningful grants, loans, and other financial incentives for accelerating widespread adoption of HIT systems and tools are essential for accelerating widespread adoption of HIT.

We commend you for your legislative proposal to establish an HIT Resource Center to provide technical assistance and serve as a forum to exchange knowledge and experience in order to support and accelerate efforts to adopt, implement, and effectively use interoperable HIT.

Conclusion

Despite the complexity and cost of developing an interoperable, nationwide HIT infrastructure, physicians realize the transformative power that adoption of this technology promises for the future of patient care. The AMA appreciates the leadership of the Subcommittee and remains committed to working closely with you on further developing legislation in order to accelerate the widespread adoption and implementation of HIT.

"Discussion Draft of Health Information Technology and Privacy Legislation"
American Medical Association
June 4, 2008

Summary

The American Medical Association (AMA) commends Chairman Pallone, Ranking Member Deal, and Members of the Subcommittee on Health for recognizing the importance of moving toward an interoperable, nationwide HIT infrastructure and the crucial role the federal government has in assisting the health care industry to accelerate the adoption and implementation of HIT systems and tools. When implemented properly in a connected environment, widespread HIT adoption will transform the practice of medicine and provide physicians with a powerful tool by putting real-time, clinically relevant patient information and up-to-date clinical decision support tools in practitioners' hands at the point of care. Physicians agree that HIT is a means to improve patient safety, advance care coordination, and increase administrative efficiency. In order to achieve this reality, a coherent HIT environment will need to be highly connected, secure, affordable, and be integrated into the typical workflow of medical practices as diverse as those in large hospitals, community health centers, and among rural solo practitioners.

A Connected HIT Environment. Perhaps the largest impediments to the effectiveness of HIT are the lack of interoperable standards and systems and connectivity of health care data among health care providers. Currently, most health care data, whether on paper or electronic, are trapped in "silos." As a result, a patient may have a physician or health system that uses HIT, but if that patient requires care elsewhere, the information from that system may not be accessible. Therefore, the real benefits of HIT will only be realized in a highly networked environment in which data is liberated from those silos and shared appropriately with health care providers. Moreover, the current myriad of federal initiatives should be coordinated to avoid conflicts and the duplication of efforts. We agree with your proposal that each agency focus on areas of its greatest expertise and technical capability. Current government initiatives and advisory committees should incorporate greater physician representation and involvement, since physicians will use and are expected to invest most heavily in these advanced systems.

Privacy and Security of Patient Health Information. The AMA urges policymakers to make privacy and security of patient medical information a top priority. Gaps in federal privacy protection coverage leave large volumes of identifiable health information vulnerable to improper access and disclosure without meaningful enforcement mechanisms or remedies. Forming a national health information infrastructure without adequate federal privacy protections threatens not only the privacy of patients, but also the viability of such a system. Therefore, we appreciate your efforts to expand the HIPAA Rules to directly cover additional parties involved in the electronic exchange, storage, use, or handling of health information that are not currently covered by HIPAA.

Financial Incentives to Spur HIT Adoption. Although lack of interoperability and cost savings are barriers to physician adoption as they significantly reduce the clinical and business case for physician HIT investment, direct and indirect HIT costs are also an impediment, particularly for physicians practicing in small office settings. The AMA strongly believes that meaningful grants, loans, and other financial incentives for acquiring, implementing, maintaining HIT systems and tools are essential for accelerating widespread adoption of HIT.

Mr. PALLONE. Thank you, Dr. Stack. Dr.—is it Thames or Thames?

Dr. THAMES. Thames, Mr. Chairman.

Mr. PALLONE. Thames. Thank you.

STATEMENT OF BYRON THAMES, M.D., MEMBER, AARP BOARD OF DIRECTORS

Dr. THAMES. Mr. Chairman, members of the Committee, my name is Byron Thames. I am a physician and a member of AARP's Board of Directors. Thank you for holding this hearing on one of AARP's highest priorities, enacting legislation to promote health information technology this year.

Health IT is an essential building block for health reform with enormous potential to improve the effectiveness and efficiency of health care. We commend Chairman Dingell and Ranking Member Barton for crafting thoughtful, bipartisan draft legislation. This marks real progress towards our goal of enacting health IT legislation this year which we shared with a broad range of stakeholders. In fact, the need for health IT is one of the first areas of consensus AARP found with our allies, and Divided We Fail is a nonpartisan effort led by AARP, the Business Roundtable, the National Federation of Independent Business and Service Employees International Union, to ensure that all Americans have access to affordable quality health care and financial security.

Consumers want the vast benefits health IT can provide for many reasons. Health IT can help us reduce medical errors, saving both lives and money. It can provide access to comprehensive medical records any time, anywhere. It can eliminate the need for redundant tests and paperwork. It can help to engage consumers in managing their own care. It can help us to quickly identify public health threats and the most effective, efficient ways of providing care.

Health IT also can enhance privacy protections in many ways. Today's paper-based records allow anyone who can gain access to the files to share sensitive information with little chance of detection. Health IT can establish firewalls and leave an audit trail of who accessed or altered sensitive, personal health data.

Health IT also raises new privacy concerns. The potentials for breaches, data mining, and misuse of sensitive data is real and could undermine consumer confidence in health IT unless we have privacy rules that consumers can trust. But we should not be forced to choose between health IT and privacy.

We also need to be pragmatic in how we address privacy. Requiring consent anytime records are shared may sound reasonable at first, but would be unworkable in practice. It also could have unintended consequences like promoting blanket consent forms that weaken protection and create a false sense of security.

What we need instead is a package of privacy policies that limits data collection and use, ensures patients access to information, and provides rigorous user authentication and other appropriate mechanisms to address security.

Because establishing workable privacy protections is so complex, AARP believes the best approach is that taken in the Dingell-Barton draft legislation. It establishes a framework, including basic

protections such as requiring that people be notified if their privacy is breached. It then leaves more detailed privacy policies to an advisory board operating under Federal Advisory Committee Act rules that ensure openness and accountability. The Dingell-Barton discussion draft also provides grants to providers who are small, rural, nonprofit, or serving underserved communities. This is essential for ensuring that underserved communities reap the full benefit that help IT promises in improving quality and reducing health disparities.

So, again, we commend this committee for its leadership on this vital issue. We look forward to working with you to ensure passage of health IT legislation this year; and at the appropriate time, I will be happy to answer any questions. Thank you very much.

Mr. PALLONE. Thank you, Dr. Thames.

[The prepared statement of Dr. Thames follows:]

TESTIMONY

BEFORE THE SUBCOMMITTEE ON HEALTH

OF THE

HOUSE ENERGY AND COMMERCE COMMITTEE

ON

PROMOTING HEALTH INFORMATION TECHNOLOGY

June 4, 2008
WASHINGTON, DC

WITNESS: BYRON THAMES, M.D.
AARP BOARD OF DIRECTORS

For further information, contact:
Paul Cotton
Federal Affairs Department
(202) 434-3770

On behalf of AARP's nearly 40 million members, I want to thank you for holding this hearing on one of our highest priorities this year – advancing use of information technology (IT) to improve our health care system. Health IT has enormous potential to improve the safety, effectiveness, and efficiency of care. It is an essential building block for health reform.

AARP believes it is essential for Congress to enact Health IT legislation this year. We commend Chairman Dingell and Ranking Member Barton for crafting thoughtful, bipartisan draft legislation for discussion, which marks real progress in achieving this important goal.

Consumers want the vast benefits Health IT can provide. Health IT can:

- Reduce medical errors that, according to the Institute of Medicine, result in an estimated 98,000 people in hospitals each year;

- Provide access to comprehensive medical records anytime and anywhere, including emergencies when people cannot speak for themselves;

- Reduce the need for duplicate tests and procedures now commonly performed because records are not available;

- Eliminate redundant paperwork burdens and the need for patients to repeat medical history and demographic data over and over;

- Reduce health disparities in minority and low-income populations by giving people in underserved communities access via telemedicine to treatment they otherwise might not receive, given the lack of adequate numbers of health care professionals and facilities in rural and inner city areas;

- Engage consumers in managing their own care and facilitate a wide array of technologies that help people stay in their own homes and out of institutions;

- Allow caregivers and providers to better coordinate care and spend more time with patients and less time on paperwork;

- 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 public health threats and the most effective, efficient ways of providing care.

In addition to these quality improvements, estimates are that HIT could save billions of dollars. The Congressional Budget Office has noted that potential savings are highly dependent on how widely and how well we implement and integrate Health IT into our health care system. Their recent report underscores the need for legislation to promote widespread adoption and ongoing efforts to advance appropriate utilization to maximize the potential quality improvements and cost savings.

Privacy

Health IT can enhance privacy protections in many ways, but it also raises new concerns that we must address as we move forward with Health IT. Today's paper-based records allow anyone who can gain access to the files to see, copy and share sensitive information with little chance of detection. Health IT can establish firewalls, requiring passwords and permission to gain access, and leave an audit trail of who accessed or altered the data.

Health IT also can allow people with heightened privacy concerns to easily identify subsets of their records that they do not want shared, such as those for mental health, HIV/AIDS, reproductive health, and other sensitive data.

However, electronic records have potential for breaches, data-mining, and misuse of sensitive data that could undermine consumer confidence in Health IT. If privacy protections are inadequate, consumers may withhold information and forego treatment to avoid embarrassment and discrimination.

For Health IT to thrive, we need privacy rules that consumers can trust. But we also need to be realistic and pragmatic. Simplistic approaches like requiring consent any time records need to be shared may sound reasonable at first, but may be unworkable in practice, have unintended consequences like 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, such as limiting data collection and use, ensuring patients' access to information, and providing rigorous user authentication and other appropriate mechanisms to address security.

Because of the complexity of establishing workable privacy protections, AARP believes the best approach is to have Health IT legislation charge an advisory board, established under Federal Advisory Committee Act rules, with developing the bulk of needed privacy policies. This ensures openness and accountability in the development of recommendations for privacy rules. Given Congress' long history of being unable to come to consensus on health privacy rules, this is probably the most prudent approach to advancing both privacy and Health IT.

But clearly, given Health IT's enormous potential to improve quality and efficiency, we should not be forced to choose between Health IT and privacy.

And, despite outstanding privacy concerns, there is broad support among a majority of the American public for advancing Health IT. 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, which Health IT can facilitate.[1]

Divided We Fail

Divided We Fail is a non-partisan effort to ensure that all Americans have access to affordable, quality health care and financial security. It is lead by AARP, The Business Roundtable, National Federal of Independent Business, and Service Employees International Union, and supported by more than 70 other organizations ranging from Consumers Union to Disabled American Veterans and the Republican Main Street Partnership.

Divided We Fail believes individuals, businesses and government all have a part to play in finding common-sense, non-partisan solutions for affordable, quality health care and lifetime financial security. One of our goals in 2008 is to ensure that our leaders make public commitments to make working toward real solutions to health and financial security issues a top priority. Health IT, with its enormous potential to improve the quality and affordability of health care, precisely fits our Divided We Fail agenda. In fact, Health IT is one of the first areas of consensus AARP found with our allies in our Divided We Fail effort.

---

[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

The Promoting Health Information Technology Act

The four lead organizations in DWF have jointly endorsed the "Promoting Health Information Technology Act," (H.R. 3800) introduced by Energy & Commerce Committee members Anna Eshoo (D-CA) and Mike Rogers (R-MI), and co-sponsored by Committee members Marsha Blackburn (R-TN), Eliot Engel (D-NY), Edolphus Towns (D-NY), Mike Ferguson (R-NJ), and Bart Stupak (D-MI). The Promoting Health Information Technology Act shares some of the following key policies with the Dingell-Barton discussion draft bill that we believe should be part of any Health IT legislation this Committee considers:

- Promotes faster development of necessary standards, such as for "interoperability" that will allow different Health IT systems to exchange information nationwide, by codifying and strengthening the Office of the National Coordinator and the American Health Information Community (AHIC) that makes policy recommendations for these standards, and giving AHIC a specific charge to address privacy polices that must be built into these standards.

- Requires notification to individuals when the privacy of their sensitive health information is breached.

- Provides grants and loans to small, rural, inner city, and non-profit providers who need financial assistance to adopt Health IT.

- Provides, with strict beneficiary privacy protections, much-needed access to physician-specific Medicare claims data. This is essential for maximizing the ability to identify high-quality and efficient practice patterns, and promoting cost control strategies that improve rather than compromise quality.

Dingell-Barton Discussion Draft

The draft bipartisan legislation that Committee Chair Dingell and Ranking Member Barton have provided for discussion is thoughtfully crafted and includes many similar important provisions listed below.

- Establishes in law the Office of National Coordinator, as well as a Health IT Policy Committee and HIT Standards Committee. These committees would both be governed by Federal Advisory Committee Act rules that ensure openness and accountability, and include consumers and other stakeholders to develop recommendations for interoperability and other needed standards.

- Assigns the Policy Committee a specific charge to address privacy, and instructs the Standards Committee to follow Policy Committee recommendations.

- Requires notification to individuals when their privacy is breached, and includes several additional provisions that clarify and strengthen privacy policies in existing regulations, for example by stating that providers must honor patient requests to not share health information with insurers for payment purposes if the patient pays for care out of pocket.

- Provides grants to hospitals, health clinics, and physician practices that are small, rural, non-profit or serving underserved communities who need financial assistance to adopt Health IT, as well as funds to states and tribes to develop additional loan programs, and additional funding for regional health information exchange initiatives. This funding is essential for ensuring that

- medically underserved communities reap the full benefit that Health IT promises in improving quality and reducing disparities.

The Dingell-Barton discussion draft does not, in its present form, provide needed access to physician-specific Medicare claims data that is essential for identifying the most effective and efficient practice patterns. Access to this data will help in crafting additional health reforms that bring runaway health care inflation under control without compromising quality. AARP is interested in working with the drafters to provide access to this vital information through the bill or address it in additional legislation as soon as possible.

Conclusion

If Health IT legislation is not enacted, our health care system will continue to be mired in paperwork. Thousands of lives and billions of dollars will be needlessly lost. Consumers will continue to be harmed by the failure to have their vital information in the hands of those who care for them, and inconvenienced by the need to fill out redundant forms. Doctors and nurses will still have to struggle to get complete information about their patients and waste time on paperwork that would be better spent on patient care. We deserve better.

AARP commends Chairman Dingell and Ranking Member Barton for their thoughtful, bipartisan discussion draft legislation, and we look forward to working with members of this Committee and all of Congress to ensure passage of strong Health IT legislation this year.

Mr. PALLONE. Ms. Dare.

STATEMENT OF FRANCES DARE, DIRECTOR, CISCO INTERNET BUSINESS SOLUTIONS GROUP

Ms. DARE. Mr. Chairman, Ranking Member, members of the subcommittee, my name is Frances Dare, and I am Director of the Healthcare Consulting Practice for Cisco's Internet Business Solutions Group. My colleagues and I work with Cisco's health care customers to transform their organizations both with advanced technologies and with business process innovation. I am pleased to be here today to offer Cisco's views on the HIT legislation the subcommittee will consider.

Cisco has a very strong commitment to health care not only as a technology company serving our customers, but as a self-insured employer. We provide health insurance coverage and health benefits to more than 90,000 U.S.-based employees and their dependents.

HIT is an essential enabler of U.S. health transformation, and Cisco's vision is a world of connected health that creates collaborative relationships among all stakeholders to enable safe, affordable, and accessible health care. Connecting people with interoperable processes and technologies, connected health provides critical information and health services anywhere, anytime.

HIT alone does not solve all of health care's challenges, but few of the problems facing health care can be solved without health care as a critical enabler.

We favor legislation that promotes and even accelerates the adoption of HIT. Legislation at this time can help reignite momentum for a national HIT agenda. The draft bill speaks to many of the key elements needed for successful industry transformation, and my written comments address many of the bill's key provisions.

This morning I would like to spend just a couple of minutes highlighting the importance of the Federal Government's purchasing power and its own HIT investment strategy. As members of the subcommittee know, the Federal Government is the largest single health care purchaser of health care in this country. As such, it should be the Nation's most committed and sophisticated HIT consumer. It becomes the best custodian of tax dollars when Federal agencies purchase standards-based technologies to administer or sponsor health programs.

We support the draft provision that requires agencies to buy standards-compliant technology systems as they implement, upgrade or acquire HIT. With the Federal purchasing requirement, the Federal Government essentially aggregates demand and coalesces the market in an otherwise fragmented industry. When the largest single customer in any industry—and for U.S. health care, that is the Federal Government—brings the industry together and endorses investments and standards-compliant IT, it reduces market uncertainty, and that spurs investment by private sector technology companies.

The government's spending requirements in the draft bill focuses on HIT use for the direct exchange of individually identifiable health information. We encourage revisions to make the draft con-

sistent with the Eshoo-Rogers bill language that includes HIT for clinical care and also for the electronic retrieval or storage of health information. Private sector support for HIT standards and certification is clear from the success of the certification commission for health care information technology, otherwise known as CCHIT. More than 40 percent of ambulatory EHR vendors, representing an estimated three-quarters of total EHR market penetration, receive CCHIT certification in the first year, voluntarily participating.

The Federal Government also has an opportunity to accelerate market forces using other incentives to promote HIT. We recommend the national coordinator work with the Secretary of HHS and the Director of CMS to create forward-thinking reimbursement policies, for example, Medicare reimbursement for remote consultations between physicians and their patients utilizing secure messaging technologies. As well, telemedicine solutions and other HIT can really redefine access to care when reimbursement practices recognize the services provided and the treatment rendered regardless of location, rather than time reimbursement to specific clinical settings such as physician practices.

Before closing I would like to highlight one other key topic. Americans do remain concerned that their health information could be vulnerable to misuse. Federal legislation should create a clear trigger for notification when a breach of protected health information presents a reasonable risk of significant harm, medical fraud, identity theft, or other unlawful contact.

Technology vendors continually develop solutions to make patient data more secure. The draft legislation recognizes that security measures should create presumption of no reasonable risk if unusable data is breached. We encourage Congress to fully address the need to render data unusable rather than requiring specific technologies such as encryption.

In closing, we urge the Committee and the House to take up the draft legislation in the coming weeks. We commend the Chairman and Ranking Member for drafting a strong bipartisan draft that can be enhanced through the legislative process and passed into law this year. Thank you.

Mr. PALLONE. I thank you, Ms. Dare.

[The prepared statement of Ms. Dare follows:]

Frances Dare
Director, Healthcare Consulting Practice
Internet Business Solutions Group
Cisco
June 4, 2008
U.S. House of Representatives
Committee on Energy and Commerce - Subcommittee on Health

Mr. Chairman, Ranking Member Deal, Members of the Subcommittee:

My name is Frances Dare, and I am director of the healthcare consulting practice for the Cisco Internet Business Solutions Group (IBSG). I work with Cisco's major healthcare customers to innovate and transform their organizations with intelligently applied advanced technologies and business process innovations. I am pleased to be here today to offer Cisco's views on the healthcare IT (HIT) legislation the Subcommittee will consider in the coming weeks.

Cisco was founded 24 years ago by two computer scientists at Stanford University who were seeking a way to exchange information among different computer systems in two different departments. At that time, such communication was difficult, if not impossible—even within a college campus. Today it is, of course, common across the world. Our founders developed a device to enable communication among their disparate computer systems. Known as a router, this became the first Cisco product. Today we are a leading supplier of Internet equipment and advanced technologies. We employ more than 30,000 people in the United States, and our headquarters is in San Jose, California.

Networking equipment—routers and switches—forms the core of the global Internet and most corporate, government, and healthcare networks. Cisco develops the equipment that makes the Internet and networking work. Healthcare providers, payers, and life sciences companies all depend upon Cisco products to move information within their organizations; share information across their business ecosystems; enable their employees to collaborate using video, voice or data; increase productivity through the use of wireless technology; and ensure the security of their networks.

Cisco has a strong commitment to healthcare—not only as a technology company serving our customers, but also as a self-insured employer purchasing health services and providing health benefits for more than 90,000 U.S.-based employees and dependents. Like others, we have seen healthcare costs increase at a rate of 8 to 11 percent annually in recent years.

In partnership with other employers, providers, technology companies, and payers, we are active with initiatives that address healthcare cost and inefficiency. Examples include The Silicon Valley Pay-for-Performance Consortium. The consortium was begun in 2005 by Cisco, Intel Corporation, and Oracle, along with a number of leading California physician organizations and Cigna, to accelerate use of technology for quality healthcare. Through this consortium, seven San Francisco Bay Area provider organizations representing 25 practice sites and more than 1,800 physicians accepted the invitation to join and continue to participate. We are also a leader in the Continua Health Alliance,

whose mission is to establish an ecosystem of interoperable personal telehealth systems that empower people and organizations to manage their health and wellness more effectively.

HIT is an essential enabler of U.S. health transformation. Lives can be saved, equal healthcare access achieved, and costs reduced with information technology adopted broadly among all involved with health and health services. The best outcomes occur when IT is integrated into healthcare operations, transactions, and services. The adoption of modern HIT, including electronic health records (EHRs), is widely recognized as having the single greatest potential for reducing healthcare costs and improving the quality of care.

The American healthcare system is plagued by rising costs and declining quality of care:

- Medical care remains focused on episodic treatment of disease and injury despite demographic trends that demand lifetime health coordination and better management of the more than 90 million Americans who live with chronic illnesses. The medical costs associated with their care are more than $510 billion per year.
- Americans receive recommended, evidence-based care only about half the time. One study estimates that 30 percent of all healthcare dollars are spent on inappropriate care. Clinicians practice expensive care needlessly due to a lack of easy reference information and decision support tools.
- Preventable medical errors are the eighth-leading cause of death in the United States. The Institute of Medicine estimates 45,000-98,000 people die every year from

hospital medical errors—more than perish from motor vehicle accidents or breast cancer.

HIT alone does not solve all of healthcare's challenges, but few of the problems facing healthcare can be fixed without HIT as the essential enabler. HIT can transform the healthcare industry by enabling clinical best practices, enhancing the delivery of health services, and redefining the point-of-care. The result is improved collaboration across the continuum of care, greater health worker efficiency and effectiveness, empowered consumers, and increased consumer accountability.

Cisco's vision is a world of "Connected Health" that creates collaborative relationships among all stakeholders to enable safe, affordable, accessible healthcare. Connecting people with interoperable processes and technology, Connected Health provides critical information *and* health services anywhere, anytime.

We favor legislation that promotes, even accelerates, the adoption of HIT. Integrating the Federal Government's role in HIT promotion is a shared goal. Legislation at this time can help re-ignite momentum for a national HIT agenda.

The successful transformation of the U.S. healthcare system through the adoption of HIT depends upon the presence of several key elements: strong national leadership; input from multiple stakeholders; interoperable solutions based upon recognized industry standards; incentives for adoption; and fair privacy practices and security requirements.

We believe the legislation you will consider contains provisions that address all of these critical elements.

We support legislative efforts to make the Office of the National Coordinator for Health Information Technology (ONCHIT) permanent and provide adequate funding to fully cover the operational needs of the Office. We are also pleased to see the requirement for the National Coordinator to report results annually to keep Congress engaged. We encourage Congress to include in ONCHIT's charter responsibility for accelerating the adoption of HIT and developing a strategic plan that incorporates a range of technologies—an EHR for every American by 2014, as well as solutions such as electronic prescribing, secure messaging, and remote monitoring technologies that support health and wellness.

The development of a strategic plan to implement a nationwide HIT infrastructure cannot be successful unless the Office of the National Coordinator has input from all stakeholders, including patients, doctors, hospitals, clinics, payers, consumer advocates, public health professionals, and the HIT industry. We're pleased to see that Congress specifically calls for broad representation on the HIT Policy Committee as envisioned in the legislation, as each stakeholder has important expertise to share and unique insights to offer.

We are also glad that the HIT Policy Committee is empowered to consider telemedicine solutions as well as technologies for remote monitoring, as well as those that support

continuity of care. We would like to encourage Congress, ONCHIT, and the policy committee to consider those solutions in the broadest sense of their application, without placing constraints on the target population or their potential uses.

The National Alliance for Health Information Technology has defined interoperability in the following way:

"Interoperability is the ability of different information technology systems and software applications to communicate; exchange data accurately, effectively, and consistently; and use the information that has been exchanged."

HIT must be interoperable to be effective. We fully support the call for interoperable IT and standards development. A nationwide health IT network will achieve its maximum benefit only if health information can be shared freely and securely across the continuum of care.

Many providers—particularly those in small practices—face a real challenge as they struggle to make a business case for HIT adoption. Not only must they decide on the most cost-effective means of integrating IT into their practices; they must also determine if the solution they choose will allow them to communicate with others. The reluctance of some to invest in HIT will be overcome only if providers can be assured that the solutions they purchase are certified interoperable and meet industry standards.

As members of the Subcommittee know, the Federal Government is the largest single purchaser of healthcare, spending close to 45 cents of every healthcare dollar. The Federal Government must play a leading role in driving adoption of interoperability standards and facilitating certification of interoperable technologies. The standards committee envisioned in the legislation will bring the proper representatives together to identify and recommend consensus-based standards the government itself can, and should, use.

We're pleased to see that the legislation directs the Federal Government to use its market power to drive implementation of standards by mandating their use by federal agencies. We support enactment of this provision both in the context of the Federal Government's procurement of HIT solutions and in its contractual arrangements with private entities providing services to the government. While use of these standards will not be required, it should be encouraged. The Federal Government can set an example for other payers of the benefit of embracing standards.

One of the biggest obstacles to broader use of HIT is the lack of financial incentives for providers. Financial benefits brought about by HIT investment will, for the most part, flow to payers and patients, rather than to providers, in the form of savings brought on by fewer duplicative tests and medical errors. While many providers can and will invest, small practices—especially those in rural and underserved areas—will face financial challenges investing in HIT solutions. The bill recognizes the need for the government to

provide help through demonstration projects, loans, and grants. We applaud these initiatives and encourage the maximum appropriations possible.

We also believe the Federal Government has an opportunity to accelerate market forces using targeted investments and incentives to promote HIT. We recommend the National Coordinator work with the Secretary of HHS and the Director of the Centers for Medicare and Medicaid Services to create forward-thinking reimbursement policies. For example, establish Medicare reimbursement for remote consultations between primary care physicians and patients, supported by secure messaging.

In countless surveys many Americans remain concerned that their medical information could be vulnerable to theft or that it is being shared without their knowledge. The bill recognizes this by strengthening patient privacy protections and security requirements in an environment where patient data is shared electronically. It codifies, in a manner consistent with the Health Insurance Portability and Accountability Act, the use of safeguards for securing patient data, and also requires notification when a patient's data is stolen. Federal legislation should create a clear threshold that requires notification when a breach of personally identifiable health information presents a reasonable risk of significant harm, medical fraud, identity theft or other unlawful conduct.

Innovative HIT solutions are being developed daily to make patient data more secure than ever before, including when records were maintained only in paper form. Audit trails, authorization and authentication requirements and rendering data unusable are just

a few tools that make electronic patient data more, not less secure, than paper-based patient data. We are pleased the draft legislation recognizes that security measures can and should create a presumption that no reasonable risk exists if unusable data is breached. However, we would encourage Congress to fully address the need for rendering data unusable rather than simply requiring encryption. As noted in the legislation, the Federal Trade Commission is well suited to determine the tools and application of such tools with respect to rendering data unusable or indecipherable.

In closing, we urge the Committee and the House to take up the draft legislation in the coming weeks for consideration. We believe the draft bill addresses five key elements: strong national leadership; input from multiple stakeholders; interoperable solutions based upon recognized industry standards; incentives for adoption; and fair privacy practices and security requirements. We commend the Chairman and the Ranking Member for drafting a strong bi-partisan discussion draft that can be enhanced through the legislative process and hopefully passed into law this year.

Overview of Cisco testimony
Frances Dare
Director, Internet Business Solutions Group
June 4, 2008

Strong national leadership:

- Give ONC responsibility for accelerating the adoption of HIT and developing a strategic plan that incorporates a range of technologies—an EHR for everyone by 2014, e-prescribing, secure messaging, and monitoring technologies.

Input from multiple stakeholders:

- Developing a strategic plan requires the input from all stakeholders, including patients, doctors, hospitals, clinics, payers, consumer advocates, public health professionals, and the HIT industry.

Interoperable solutions based upon recognized industry standards:

- Providers need to be assured that the solutions they purchase are certified to meet industry standards.
- The Federal Government must play a leading role in driving adoption of interoperability standards and facilitating certification of interoperable technologies.

Incentives for Adoption:

- The federal government should use its market power to drive implementation of standards by mandating their use by federal agencies.
- ONC should work with CMS to develop forward-looking reimbursement policies.

Security and Privacy:

- Legislation should create a clear threshold that requires notification when a breach of personally identifiable health information presents a reasonable risk of significant harm.
- Security measures can and should create a presumption that no reasonable risk exists if unusable data is breached.

Mr. PALLONE. Mr. Reed.

STATEMENT OF MARC C. REED, EXECUTIVE VICE PRESIDENT, CORPORATE HUMAN RESOURCES, VERIZON COMMUNICATIONS GROUP, INC.

Mr. REED. Good morning, Mr. Chairman, Congressman Deal and members of the Committee. My name is Marc Reed, and I am the Executive Vice President of Human Resources for Verizon Communications. I am pleased to be here today to offer my company's support for and comments for the draft health information technology and privacy legislation.

With nearly a quarter of a million employees plus dependents and retirees, Verizon Communications provides health care to approximately 900,000 Americans at an annual cost of about $4 billion. We have a very big stake in creating a high quality health care system that is both affordable and accessible. For us, health IT must be a critical piece of such a system, and our actions demonstrate our commitment.

Verizon has been involved in a number of critical efforts to accelerate health IT including participating in the Federal Commission's Systemic Interoperability, the American Health Information Community, the Health IT Now! Coalition and through the Business Roundtable's Consumer Health and Retirement Initiative.

But perhaps the best demonstration of our support of health IT is that we have implemented elements of health IT for our employees. The Verizon HealthZone initiative is an electronic personal health records system providing employees and their family members with tools and resources to help make well-informed decisions about their health care. We believe that the more you know about your health, the better you can improve, maintain and manage it.

Health care is one of the few segments of the American economy not to have been transformed by modern, efficient information technology. My written testimony outlines the benefits of health IT. Your commitment to drafting the legislation demonstrates that you understand the value it will offer.

Now I would like to comment on the key components of the draft legislation you have circulated. We support the following items that are contained in the draft legislation.

First, we support development of uniform interoperable standards. This draft legislation codifies the work of the Office of the National Coordinator in its role in establishing the strategy to develop and implement the standards for interoperability. We support this. We believe that this effort should build upon the work.

Second, standards must be developed with the establishment of two different advisory committees. One group of expert stakeholders should provide policy input to the appropriate bodies. The second group should be a public-private partnership of key purchasers and others who can influence the setting of standards. There currently is an effort to form AHIC 2.0, and we would ask Congress to be cautious about delaying these current activities.

Third, there must be support for adoption of those standards so that providers and payers know the systems in which they invest will communicate with each other. We support the Federal Government's using their purchasing power to promote adoption of stand-

ards and allowing the Centers for Medicare and Medicaid Services to have the authority to adopt these standards.

Fourth, we support a voluntary certification process to ensure systems meet the standards.

Fifth, we believe it is important that providers who cannot afford to buy these systems have access to grants or loans. This assistance should be a last resort, but it is necessary to ensure we have uniform adoption nationwide.

In terms of privacy and security, we applaud the bill's addressing of accountability and enforcement. We believe that Federal law should be authorized to establish and enforce security standards so that private health information is protected through encryption or firewalls or the most up-to-date security available. If someone intentionally breaks into these systems, they should be punished and enforcement should be at a national level.

Because Verizon is an international company with business operations in all 50 States, we strongly encourage the Committee to create a uniform notification process that Verizon can follow regardless where the disclosure occurs, by preempting conflicting State breach laws.

I urge all Members of Congress to vote to enact this legislation this year. Passage will be a big step forward toward creating the 21st century health system that America needs.

I look forward to working with the members of the committee as you move forward on this issue. Thank you.

Mr. PALLONE. Thank you, Mr. Reed.

[The prepared statement of Mr. Reed follows:]

Testimony of Marc C. Reed

Verizon Communications Inc.

Before the House Committee on Energy and Commerce, Subcommittee on Health
"Discussion Draft of Health Information Technology and Privacy Legislation"

June 4, 2008

Introduction

Good morning, Mr. Chairman, Congressman Deal and members of the Committee. My name is Marc Reed, and I am the Executive Vice President of Human Resources for Verizon Communications. I am pleased to be here today to offer my company's support for and comments on the draft Health Information Technology and Privacy legislation.

In particular, I will touch on three matters:

First, I will give you an overview of Verizon's perspective on Health Information Technology, also known as Health IT, and the specific benefits of the system; Next, I will comment on key components of the legislation under consideration today; Finally, I will discuss the need to immediately address privacy and security concerns so we can sooner receive Health IT benefits including better quality of care and a dramatic reduction in lives lost due to medical error.

I am pleased that support for Health IT may be reaching critical mass in Congress. I hope that this hearing today brings us one step closer to a bipartisan victory—because the support is certainly out there. There are many leaders in Congress who support Health IT legislation. Bipartisan legislation sponsored by Senators Kennedy and Enzi, the Wired for Health Care Act, is pending action by the full Senate.

We at Verizon applaud and encourage the leadership of this Committee in finding common ground on this issue and bringing it the much-needed attention it deserves, and I urge you to build on this effort with swift action toward passage.

An Overview of Health IT

It is important that we as a country incorporate modern information technology into our health care system for the benefit of patients and their families, just as business and industry have adopted these technologies to the benefit of their customers. Banks use ATMs and networked computers to give us access to our financial records anytime, anywhere, and always with security and privacy. Online retailers know which books we ordered last month, and what color sweater we ordered for Christmas last year. In the same way, doctors and hospitals ought to be able to access our up-to-date health records, with our permission, whenever the situation demands.

Yet our health care system lacks even the most basic foundation for effective electronic communications. Like others who have studied this matter, we at Verizon believe Congress should act now to pass health information technology legislation, bringing significant benefits to all, on a foundation of interoperable standards and strong security requirements to protect private health information. This historic success would be the fruition of hard work by this and previous Congresses, the Administration, and the bipartisan efforts of Democrats and Republicans.

With nearly a quarter of a million employees, plus dependents and retirees, Verizon Communications provides health insurance coverage to approximately 900,000 Americans at a cost of around $4 billion a year. We have a very big stake in creating a high-quality health care system that is both affordable and accessible.

For us, it's obvious that Health IT must be a critical piece of such a system, and our actions demonstrate our commitment. Verizon CEO Ivan Seidenberg has been involved in a number of critical efforts to lay out the strategic roadmap and benefits of Health IT. For instance, he was appointed to the Federal Commission on Systemic Interoperability, which issued the October 2005 report, "Ending the Document Game: Connecting and Transforming Your Health Care Through Information Technology." This report outlined the many benefits of Health IT, and described both challenges and solutions to implementing such a system.

In addition, Verizon is an active participant in a number of important groups to promote legislation to accelerate deployment of this technology. These groups include the Health IT Now! Coalition, whose members come from about 50 organizations from across the political spectrum, including unions, employers, professional associations, consumer advocacy groups, health care professional associations, coalitions fighting disease, hospitals, clinics, retiree organizations, and insurers.

Verizon is also active through Mr. Seidenberg's Chairmanship of the Business Roundtable's Consumer Health and Retirement Initiative, as well as the Divided We Fail Coalition, which also includes AARP, Service Employees International Union (SEIU), and the National Federation of Independent Business (NFIB).

But perhaps the best demonstration of our support for Health IT is that we have implemented elements of Health IT for our employees. The Verizon HealthZone initiative is a personal health record system providing employees and their family members with tools and resources to help them make well-informed decisions about their health. We believe that the more you know about your health, the better you can improve, maintain and manage it.

The Verizon HealthZone Web site, powered by WebMD®, provides personalized and confidential health care tools and resources that can help individuals set goals for their health, and help them make the best health and health care decisions. The Verizon HealthZone tools include access to a health risk assessment, a medical condition information center, online condition management programs, and an electronic Personal Health Record where each individual can store his or her health information with security and privacy.

The system analyzes patient information to provide timely medication and care alerts automatically. Care alerts inform employees when the care they are receiving appears to be inconsistent with best practices, also known as evidence-based medicine. The care alert system monitors for preventive screenings based on ethnicity, gender, age and other factors. The system checks for potentially dangerous drug interactions. And

while the system is secure, private and thorough, it is still easy enough to use so that patients can easily share information with anyone they choose by print, fax, or direct online access.

Benefits and Savings to the Health Care System

Health IT holds the potential to reduce medical errors, improve patient outcomes, help save lives and reduce health costs. The truth is, health care is one of the few segments of the American economy not to have been transformed by modern, efficient information technology.

According to the Institutes of Medicine, as many as 100,000 people die each year from medical errors. Many of these mistakes don't have to happen— one way to help prevent these errors is access to accurate and up-to-date electronic records and that is exactly what Health IT provides.

Health IT also improves patient outcomes, particularly for those who suffer from chronic illnesses. Such patients typically have complex medical histories and treatment regimens, and every provider they visit needs complete access to this information to provide the best and most complete care. Again, Health IT is the obvious answer, transforming an often haphazard collection of phone calls, faxes and photocopies for a simple and secure login to review every bit of critical and potentially life-saving information.

Also, Health IT has the dramatic potential to reduce health costs by reducing duplicative and unnecessary tests, preventing medical errors through the delivery of complete health records, and automatic monitoring to alert doctors and patients to potentially adverse drug interactions. According to the RAND Corporation, Health IT has the potential to save as much as $81 billion a year in efficiencies and improved health outcomes. The U.S. Department of Health and Human Services has estimated that as much as 30 percent of health costs could be eliminated through widespread adoption of Health IT.

One aspect of Health IT, the electronic health record, empowers patients to review their own records. The benefits of having access to your own information range from financial savings to potentially saving a life. For example, a Verizon employee using HealthZone found insurance claims for a condition that his doctor confirmed he did not have. After further investigation, both patient and doctor learned that the claims had been submitted in error, and they were able to work with the insurance company to adjust and clear the patient's record.

At Verizon, one of our employees wrote to us and said: *"Since it is a top priority for me to live healthily for the sake of my children, HealthZone provides a place to store my personal information, AND to track my progress toward my health improvement goals. Another great benefit of HealthZone is the drug interaction warnings. HealthZone provides a place to store my children's health information and the option to*

share that information with others. For example, at the start of each school year, I can provide the school nurse with a tailored report on each child."

There are plenty of examples out there, but the point is that when patients have more information, they have more power and more control and more choice in improving the quality of their care, the quality of their lifestyles, and thus the quality of their lives.

Verizon employees enjoy benefits of Health IT. Various insurance providers, hospitals and clinics, and other groups have implemented Health IT in various capacities, too. But everyone should have this benefit—and that will be possible only when Congress establishes a foundation in law for the rapid and widespread deployment of such a system.

Key Components of the Legislation

Next, I would like to comment on the key components of the draft legislation you have circulated. We believe that the Roadmap must include the following five key issues:

1. **Development of uniform, interoperable standards.** This legislation codifies the work of the Office of the National Coordinator for Health Information Technology (ONCHIT) and its role in establishing the strategy to develop and implement the standards for interoperability. We support this provision so long as it continues what is currently underway within the Administration. We do not want to slow down the important progress that is being made and believe we can find common ground to continue the efforts underway.

2. **Standards are developed with the establishment of two different federal advisory committees of expert stakeholders.** The difference between these groups is important. First, there is a need for a group of expert stakeholders to provide policy input to the appropriate bodies. The second group should be a public-private partnership consisting of key purchasers who can provide advise on the setting of standards. When the Commission for Systemic Interoperability was finalizing their Report, a number of purchasers, like Verizon, met with the Secretary to determine the next step in implementing the findings. We came together in agreement to form the American Health Information Community—better known as AHIC—to use the leverage that public- and private-sector purchasers have to influence our suppliers to adopt standards. There currently is an effort to form AHIC 2.0, and we would ask Congress to be cautious about becoming involved with these existing activities underway and whether they would have to "start over" or continue this process. Development of standards is time-consuming and should be non-political; no one can afford to wait for a new Administration to continue this effort.

3. **Adoption of standards.** We believe the standards should be uniform. In this way, providers and payers know that the systems they are buying will communicate with each other. We understand that this legislation would permit the Federal Government

to use their purchasing power to promote adoption of standards. We want to ensure that the Centers for Medicare and Medicaid Services has the authority to adopt these standards. This is in line with our efforts associated with AHIC today by leveraging purchasing power to spur adoption.

4. **Voluntary certification.** We support a certification process to ensure systems meet the standards. This does not have to be mandated, but can be implemented through incentives.

5. **Financial incentives.** We believe it is important that providers who lack adequate resources for the purchase of these systems have access to grants or loans. This assistance should be a "last resort," but is necessary to ensure we have uniform adoption nationwide. Our government can't afford to buy all providers systems—but we can't afford for those without the means to participate to be left behind. One of the key benefits of having national interoperability standards is that providers can purchase technology without the fear that they are picking the wrong technology. Financial assistance should be available to those providers who can demonstrate that they need the assistance.

6. **Privacy and Security.** Health IT enhances data security and privacy. Under the current paper-based systems, many can open a filing cabinet, take out sensitive patient information, even copy and distribute it, then return the papers without detection. Health IT should establish a safe firewall around patient data, requiring passwords and permission to gain access, and leaving an audit trail of who accessed the data, when and why. That is why we believe that there should be uniform security standards protecting consumers' private health information. These standards should be nationwide and should be enforceable at the federal level.

In the case of the Verizon HealthZone Web site, which is HIPAA compliant, all of the data is gathered and managed by third-party vendors, such as WebMD. Participation is voluntary, private and confidential, and Verizon does not have access to any participant data. The participant can choose to share it with third parties, including their doctor or health plan, for medical advice and consultation.

The government needs to develop interoperability standards that have well-defined objectives for electronic record management and security. This will begin to give consumers a sense of security about electronic medical records. Regulations in the banking industry give consumers the sense of confidence to transact banking business which oftentimes includes bank routing numbers, credit cards numbers and other personal indentifying information.

Let me comment on a few of the relevant provisions in the legislation:

a. **We applaud accountability and enforcement for privacy and security.** The draft legislation establishes an enforcement authority over "Business Associates" under the Health Insurance Portability and Accountability Act (HIPAA). The draft also

includes notification to patients when there is a security breach. Finally, the draft limits the current consent to treatment and payment information. In Verizon's contractual relationships with our insurers, as well as WebMD, which administers the Verizon HealthZone, we conduct periodic audits to ensure compliance with standard IT security measures.

b. **We believe that Americans should have confidence in the security of these new systems.** If someone intentionally breaks into these systems, they should be punished, and enforcement should be at a national level.

c. **Any breach of individually identifiable health information should trigger a notification to individuals whose information has been disclosed.** We support the Committee's including language in the draft to address this issue. Because Verizon is an international company with business operations in all 50 states, we strongly encourage the Committee to create a uniform notification process that Verizon can follow regardless of where the disclosure occurs by preempting conflicting state breach laws. This will ensure a transparent process for consumers whose information is inadvertently or wrongfully disclosed and certain path for companies to follow. Some of our employee health records may be kept in the same computer files regardless of the state in which they work. In addition, many of Verizon's employees cover multi-state regions in performance of their duties. The same notice of a breach should go to a Verizon employee who works in California as one who works in New Jersey.

Conclusion

In conclusion, and on behalf of Verizon, I appreciate this opportunity to encourage the Committee and Congress to swiftly pass health information technology legislation. For the health care industry to invest in and deploy Health IT, they need to know that the rules won't change. Only Congress can make such assurances.

We believe there are four things that should be done at the federal level:

- Establish federal leadership for a public-private process to set standards;
- Offer providers financial incentives to encourage the adoption of Health IT;
- Educate Americans on the value of electronic health records and information on quality of providers; and
- Protect the security of the new systems so that consumers have confidence that their private health information is protected.

Right now, Congress, the Administration, the health care industry and the public are united behind Health IT. It enjoys broad bipartisan support not only in the Congress but also among health care providers, business, labor, disease advocacy groups, medical associations and consumers. By acting now, Congress can achieve a powerful victory for all Americans by essentially just formalizing what is already agreed upon.

I urge all members of Congress to vote to enact this legislation this year. Passage will be a big step toward creating the 21st century health care system that America needs. I look forward to working with the members of this Committee as you move forward on these issues.

Mr. PALLONE. Mr. Ferguson.

STATEMENT OF JAMES A. FERGUSON, EXECUTIVE DIRECTOR, HEALTH IT STRATEGY & POLICY, KAISER PERMANENTE

Mr. FERGUSON. Thank you for the invitation to be here today. I am Jamie Ferguson, Executive Director of Health IT Strategy and Policy for Kaiser Permanente, which is the Nation's largest integrated health care delivery system with more than 8.7 million members. My work focuses on expanding our IT capabilities and interoperability both within Kaiser Permanente and with other entities in patient care and population health.

We have made significant investments in every area of health IT. We have the world's largest civilian deployment of AHR for 8.6 million people. We have implemented it in 421 medical offices, and we have deployed pharmacy and administrative functions in all of our hospitals. We have rolled out computerized physician order entry in 15 hospitals and expect to have 25 done by the end of the year.

Our early results demonstrate that health IT helps to improve care. Our online personal health record has more than 2 million active users, which is the world's largest user base of online PHRs. In addition to millions of online prescriptions and online visits, our members have had access to over 56 million lab test results, they have scheduled 2 million appointments and securely communicated with their doctors over 5 million times online.

We promote health IT interoperability, and we are core participants in federally sponsored activities such as HITSP, CCHIT, and NHIN. We also participate in health information exchange in major industry initiatives and in standards development.

Health information itself is unique. It is complex and permanent in a way that commercial or financial records are not. There is no way to create a clean slate for your personal health history. And an individual's health history may relate to family members.

Today, as you requested, I would like to offer remarks on this draft legislation.

Kaiser Permanente strongly supports the goals of this legislation. Based on our own experience, we know health IT offers great benefits, and this bill offers a framework for delivering the promise of health IT to all Americans. The bill promotes the adoption of health IT through the Office of the National Coordinator, the Health IT Policy Committee, and Health IT Standards Committee. We believe the role of the Office of the National Coordinator described in this bill covers the important duties to be undertaken.

Common standards are critical to health IT. We note that the Standards Committee both develops the standards and reviews the standards, which is unusual. Typically, the development is done by standards organizations after which the standards are adopted by a committee or an agency. We suggest that the proposed Standards Committee could endorse standards that were developed by technical panels.

Pilot testing is an excellent way to support standards adoption, and NIST is very well positioned for its proposed role in testing technical infrastructure and security, but we would question NIST having a role in establishing the certification criteria. Transitioning

AHIP to the Policy Committee is important, but other entities such as HITSP and NCVHS need transitions as well.

The bill promotes standards through Federal contracts. This contracting mechanism represents a big improvement over HIPAA in terms of speed, flexibility, and innovation. Contract provisions would require standards adoption by federally contracted health plans, but would have no requirements for providers. Providers are the primary users of electronic medical records; therefore, the contracting mechanism would be ineffective unless it adds requirements for providers to use the health IT standards.

We are especially supportive of the grants and incentives in this bill for safety net providers in underserved communities. We have committed more than $10 million in technology-related investments through community benefits.

We support the bill's intent to address the privacy and security of personal health information. All consumers should be guaranteed a minimal level of privacy and security protections, and consistent protections should apply equally to all personal health databases regardless of whether they are held by a HIPAA-covered entity or a noncovered entity. We strongly support and participate in technical innovations in this area, but different innovators who introduce substantially similar products and services should not operate under different levels of regulatory oversight.

Consumers should be notified when their personal data are breached, and our practice is to support the California Breach Notification Law. We are concerned that the bill proposes unequal breach notice for covered entities versus PHR vendors when encrypted data are involved.

The proposed restrictions on marketing practices are good so long as they do not prevent population health and patient education programs.

We look forward to working with the Committee on developing language to provide both the maximum privacy protection and clinical benefit for patients.

Mr. Chairman and distinguished members of the Committee, thank you again for the invitation to be here today. I look forward to answering any questions you may have.

Mr. PALLONE. Thank you, Mr. Ferguson.

[The prepared statement of Mr. Ferguson follows:]

KAISER PERMANENTE

Testimony of

James A. Ferguson

Executive Director of Health IT Strategy and Policy

Kaiser Foundation Health Plan

on behalf of the

Kaiser Permanente Medical Care Program

Before the

Committee on Energy and Commerce

Subcommittee on Health

U.S. House of Representatives

June 4, 2008

Chairman Dingell, Congressmen Barton, Pallone and Deal, thank you for the invitation to be here today. I am Jamie Ferguson, Executive Director of Health IT Strategy and Policy for Kaiser Permanente, which comprises the Kaiser Foundation Health Plan, Kaiser Foundation Hospitals and the Permanente Medical Groups. I am testifying today on behalf of the national Kaiser Permanente Medical Care Program. We are the nation's largest integrated health care delivery system, providing comprehensive health care services to more than 8.7 million members in nine states (California, Colorado, Georgia, Hawaii, Maryland, Ohio, Oregon, Virginia, Washington) and the District of Columbia.

For most of my six years with Kaiser Permanente, my work has focused on expanding our information technology capabilities and developing interoperability between systems both within Kaiser Permanente and across diverse entities involved in patient care and population health. Standardized health data exchange is a key to achieving benefits such as health records portability and improved coordination of care.

Background: Health Information Technology

Health information technology (IT) encompasses a broad scope of systems affecting health care. Some systems capture actual patient encounter data, such as electronic medical records (EMRs), which can include sophisticated tools for clinical decision support and electronic prescribing. Recently, the development of personal health records (PHRs) has allowed personal health data to be collected and managed in new ways; The most robust PHRs may offer the ability to make appointments, renew prescriptions, or see lab test results online. Consumers may also benefit from secure email communications with their providers through their integrated PHRs.

Health IT can also include other clinical information systems, such as laboratory, radiological and image management, pharmacy management, terminology services[1] and clinical analysis and reporting systems. Biomedical devices, including network-connected devices and home-care devices are also components of health IT. With increasing innovation, health IT can be applied to various analysis and reporting systems, leading to improved accuracy and speed in areas of bio-surveillance, public health reporting and immunization or disease registries. Health care administrative and financial information, such as claims and information derived from claims, increasingly depend on health IT.

Because of the unique nature of health information, the adoption and application of health IT imposes special challenges. Health facts and records are permanent in a way that commercial or financial records are not – there is no way to create a "clean slate" when it comes to individual personal health history. Health information is particularly sensitive because it has the potential to be misused to discriminate against individuals in employment and insurance contexts. Health records are unique to the individual; at the same time, the health history of an individual may relate to family members because certain tests, treatments, or medication may indicate genetic traits or conditions. Moreover, because of the complexity of health data, health information models are substantially more complicated than other industries' information models.

These factors present a unique combination of concerns regarding personal privacy, medical practice and liability. There are also cultural challenges of moving user groups

[1] These terminologies allow standard coding of clinical data. The National Committee on Vital and Health Statistics has been working on designating standards for clinical data and the National Library of Medicine (NLM) serves as a national release center for SNOMED CT® (Systematized Nomenclature of Medicine-Clinical Terms). The U.S. Department of Health and Human Services is beginning to require data transmission in SNOMED. http://www.ihtsdo.org/our-standards/snomed-ct/

towards adoption of health IT. Our own experience has demonstrated that all users – physicians, other providers and patients – need to attain a level of comfort and trust with the system before they are able to create value consistently using the system.

Kaiser Permanente HealthConnect™

In 2003, Kaiser Permanente began the KP HealthConnect™ project, the world's largest civilian deployment of an electronic health record. KP HealthConnect is a comprehensive health information system that includes one of the most advanced electronic health records available. It securely connects 8.6 million people to their health care teams, their personal health information and the latest medical knowledge, leveraging the integrated approaches to health care available at Kaiser Permanente.

In April of this year, we completed implementation in every one of our 421 medical office buildings, ensuring that our 13,000 physicians and all other ambulatory caregivers have full access to members' clinical information. In addition, we have completed the deployment of inpatient billing; admission, discharge and transfer; and the scheduling and pharmacy applications in each of our 34 hospitals. Now, we are in the midst of an aggressive deployment schedule of bedside documentation and computerized physician order entry (CPOE). As of today, we have 15 of our hospitals fully deployed and will have 25 completed by the end of the year.

One of our greatest lessons has been how much KP members value the ability to use online tools to manage their health. Launched in 2005, our personal health record, *My Health Manager*, now has more than 2 million active users. We believe this is the largest

user base of online personal health records in the U.S. Due to a direct link to actual clinical and operational systems, we are able to provide our members with access to robust features, including access to lab test results, appointment scheduling, prescription refills and even the ability to securely email their doctors.

To date, we have emailed members over 56 million lab test results. Our members have sent over five million secure email messages, made over two million online visits to book and review future appointments and logged over one million online visits to view past office visit information.

At Kaiser Permanente, we are already realizing the value of health IT. With 24/7 access to comprehensive health information, our care teams are able to coordinate care at every point of service – physician's office, laboratory, pharmacy, hospital, on the phone and even online. Our early results demonstrate that health IT, as *Crossing the Quality Chasm* predicted, helps to make care: safe, effective, patient-centered, timely, efficient and equitable.

Kaiser Permanente has made a huge investment in IT, both financially and philosophically. We believe it has the power to transform the way we deliver health care and improve patient health. Since the deployment of our integrated medical record, we have begun to see major advances in the ability to use information systems as a diagnostic tool (for identifying and understanding patients with certain risk factors) as well as for appropriate therapeutic intervention (for encouraging adherence and therapeutic intensification or moderation when needed).

Kaiser Permanente's Other Investments in Health IT

In addition to KP HealthConnect, Kaiser Permanente has developed and implemented other systems for administrative simplification, such as handling HIPAA claims transactions, membership enrollment, eligibility and benefits, registration and scheduling. We have other systems that provide extended clinical information capability – a panel support tool, which gives physicians more effective ways to practice preventive medicine and identify patients with specific needs. We have developed systems to support disease registries, other large scale studies and disease management.

Kaiser Permanente has been very involved in promoting health IT interoperability. We are core participants in federally sponsored activities, such as the Health Information Technology Standards Panel (HITSP), the Certification Commission for Health Information Technology (CCHIT), the National Health Information Network (NHIN) Collaboration and Trial Implementations and the National Committee for Vital and Health Statistics (NCVHS).

We also participate in local, regional and state-level health information exchange entities as well as major industry initiatives, such as the personal health record project of America's Health Insurance Plans (AHIP) and national and international interoperability standards development.

Draft Health IT Legislation

Today, as you requested, I would like to offer remarks on this draft legislation.

Kaiser Permanente strongly supports the goals envisioned by this legislation. Based on our own experiences with KP HealthConnect, we know health IT offers great benefit. We believe Congress has an important role to play in this area. This draft bill offers a framework for delivering the promise of health IT to all Americans.

The bill outlines a well-defined structure to promote the adoption of health information technology, through the Office of the National Coordinator, with the formation of the HIT Policy and HIT Standards Committees under the Federal Advisory Committees Act. We believe the role of the Office of the National Coordinator described in this bill broadly covers the important purposes to be served as well as the appropriate duties to be undertaken.

Common standards are critical to the widespread adoption of health information technology. We note that the duties of the HIT Standards Committee include development of standards as well as review and endorsement of standards, which would give the Committee an unusually broad scope. Typically, standards development is done by standards development organizations, such as HL7or IEEE, after which the standards best suited to particular purposes are selected or adopted by a committee or an agency. We suggest the Standards Committee could endorse – or select, ratify and/or recommend – standards developed by more technical panels.

Establishing a pilot-testing program as in the draft bill is an excellent way to support robust standards adoption. The National Institute of Standards and Technology (NIST) is well positioned for its proposed role in testing, and NIST should focus on its particular expertise in technical infrastructure and security. We question, however, its role in establishing certification criteria for HIT, especially given the existing role of CCHIT

Several key provisions will speed adoption of health information technology. First, the bill advocates for the adoption of uniform federal interoperability standards, mandating requirements in federal contracts. The contracting mechanism represents an improvement over the Administrative Procedures Act as applied to standards under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Contract terms and conditions allow flexibility regarding timing and enable innovation. Current and proposed versions of contract provisions, however, apply requirements for standards to all federally-contracted health plans and have no requirements for the providers who contract with those health plans. Providers are the primary users of electronic medical records and their willingness to adopt technology is crucial to the widespread promotion of health information technology. So, as a means to promote and speed EMR adoption, this contracting mechanism would be ineffective unless it adds requirements for providers to use the health IT standards.

Kaiser Permanente is especially supportive of the grants and incentives programs contained in this bill that are aimed primarily at safety net providers and small rural and community clinics that often lack the resources to purchase and maintain technology systems. As part of our mission, Kaiser Permanente works closely with community

health centers, public hospitals and health departments, supporting their efforts to provide care for the uninsured and for underserved communities with infrastructure, training, grants and equipment.

Health information technology is critical to improving the quality of health care, but the costs can be daunting for most safety net providers. Our grants help organizations make important program upgrades such as electronic patient registries. They also enable public hospitals to exchange critical information with community health centers to improve coordination of patient care. So far we've committed more than $10 million in technology-related investments to bring about a better-coordinated, safer and more effective system of care for everyone in our communities. Given tight federal budgets, a focus on the truly underserved communities is most appropriate. Competitive market pressures should serve as a catalyst for other slower adopters.

The inclusion in the bill of a transition plan to transfer the ongoing efforts and recommendations of the current American Health Information Community in a consistent manner is important. There are other entities with important roles in health information technology, which may need to be transitioned as well, including HITSP, NCVHS and CCHIT.

We support the bill's intent to address broad consumer concerns about the privacy and security of their personal information. All consumers should be able to rely on an appropriate and consistent minimum level of privacy and security protections, including consistent technical standards and rules for secondary or subsequent use of patient health data with consistent enforcement of these rules. These protections should apply equally

to all databases of personal health data, no matter where they exist in the United States. We strongly support the exploration of technical innovations aimed at providing consumers with secure choices for their health data, especially choices that allow greater capabilities, such as the ability to store and transfer data from one entity to another.

At the same time, in this rapidly evolving market, entities who offer substantially similar products and services should not be permitted to operate under different levels of regulatory oversight and enforcement. In many different health care forums we have heard concerns that non-HIPAA-covered entities that persistently store electronic personal data should be subject to the same minimum privacy and security protections as HIPAA-covered entities whether acting on behalf of consumers or as independent commercial agents.

We also agree consumers should be notified when their personal data are breached. Our general practice is to support the requirements of the California breach notification law across all of our regions. The draft bill exempts PHR vendors from notification requirements if the data in question have been encrypted. However, it does not provide the same exemption for covered entities and business associates. We are concerned about the unequal application of the notice provision and believe all entities should be held to the same rules.

We also believe that the proposed restrictions on certain marketing practices are good, so long as they do not prevent valuable population health communications about disease management, wellness programs and patient education. We look forward to working with

the committee on developing language to provide both the maximum privacy protection and clinical benefit for patients.

Mr. Chairman and distinguished members of the Committee, thank you again for the invitation to testify here today. I look forward to answering any questions you may have.

Mr. PALLONE. Dr. Elders.

STATEMENT OF JOYCELYN ELDERS, M.D., FORMER U.S. SURGEON GENERAL, CO-CHAIR, AFRICAN AMERICAN HEALTH ALLIANCE

Dr. ELDERS. Good morning. Thank you, Chairman Pallone, Honorable Ranking Member Deal and members of the Health Subcommittee. I am Dr. Joycelyn Elders, a former United States Surgeon General, the former Health Director of a rural, poor State with many underserved, less well-educated people without proper health care.

I also want to thank Congressman Towns, Ed Towns of New York, renowned for his work on this committee, including his commitment to the reduction and ultimately the elimination of health disparities and health on all fronts and across all populations.

The Committee's commitment to addressing inequities in health care for racial and ethnic communities, to addressing the needs of the uninsured and the underinsured, the disabled and the medically underserved communities including homeless and poor; I am steadfastly in support of this bill.

We can go anyplace in the world and use our card to get money out of our bank account, but you can't go across the street and have a child be able to know whether they are up-to-date on their immunizations. Most bank records, bills, personal communications, and security exchanges are currently maintained in electronic form, while the vast majority—you have heard this morning, less than 20 percent, only 18 percent in many cases—of the health information is held primarily in paper form. So I think this tells us something about our health care system.

I know that you already know that we have absolutely the best doctors, the best nurses, the best hospitals, cutting-edge research in the world, but you also know that we do not have the best health care. And, in fact, we have got a very excellent sick care system.

The problem is, we don't have a health care system; and I feel that this bill will help to serve as a connector to begin to bring together some of the multiple pieces of all of this excellence that we have to be able to impact the patients and their doctors in all segments of our population.

I am concerned about all Americans and confident that if I advocate for the most marginalized of the American people that we will secure health care of equal high quality for all. I feel that you on this committee serve as an important group to be the voice and the vision for the poor and the powerless, and also to use your tremendous power as you can in this important bill by the multiple sections that it includes to make sure that we address the needs of all populations, because very often the physicians that are serving those most in need can't afford this system. And it is very wonderful that you have included grants or low-cost loans to help those most in need and most in need of serving.

I am very encouraged by the hard work that Chairman Dingell and Congressman Pallone and ranking members have put into developing different pieces of this discussion draft and hope you use your collective wisdom to further information technology.

We are encouraged by the components of the draft, including the codification of the Office of the National Coordinator for Health Information Technology. We need someone to keep this together in order to continue its overall effectiveness for the Nation and the utilization of health information technology.

We are also encouraged by your establishment of the various advisory committees, which I feel will be very important and very critical. We like the bifurcation approach of developing standards using both policy setting committees and a Health Information Technology Standards Committee and the draft's establishment of a prominent standards development role for the National Institute of Standards and Technology.

I mentioned earlier the importance of having and establishing a resource center for education and research and setting up grant policies that I feel are very critical. We are encouraged by the provisions which call in the National Coordinator to assess and publish the impact of health information technology that this will have on the underserved community. We all know that we have a wide disparity in health care within our community, and hopefully this will provide some help. Hence, we believe that effectively applied health information technology can serve to benefit all of the American people.

Mr. PALLONE. Dr. Elders, I apologize, but if you could summarize.

Dr. ELDERS. I think the most important thing is, we very much support this bill. And we really feel that the important components are that you will make sure that it serves all of the people and that you will provide grants and the privacy pieces that are very important and critical.

Thank you.

Mr. PALLONE. Thank you very much and thank you for being here today, too.

[The prepared statement of Dr. Elders follows:]

African American
Health Alliance
healthalliance@comcast.net

Health Information Technology

Statement of

The Honorable Dr. Joycelyn Elders
Former U.S. Surgeon General
Co-Chair African American Health Alliance

Before the

House Committee on Energy and Commerce
Subcommittee on Health
June 4, 2008

African American Health Alliance --- Phone: 301-576-0845 --- Fax: 301-789-1179
Email: healthalliance@comcast.net

GOOD MORNING CHAIRMAN PALLONE, RANKING MEMBER DEAL, AND MEMBERS OF THE HEALTH SUBCOMMITTEE. I AM DR. JOYCELYN ELDERS A FORMER UNITED STATES SURGEON GENERAL – AND -- A FORMER HEALTH DIRECTOR OF A RURAL POOR STATE WITH MANY SOCIO-ECONOMICALLY DEPRIVED, UNDERSERVED, LESS WELL EDUCATED PEOPLE WITHOUT PROPER HEALTH CARE. I APPRECIATE YOUR CONVENING THIS VERY SPECIAL HEARING. I, ALSO, WANT TO THANK THE HONORABLE ED TOWNS, OF NEW YORK, RENOWNED FOR HIS WORK ON THIS COMMITTEE INCLUDING HIS COMMITMENT TO REDUCING AND ULTIMATELY ELIMINATING HEALTH DISPARITIES ON ALL FRONTS AND ACROSS ALL POPULATIONS. I, ALSO, APPLAUD THE WORK OF THE AFRICAN AMERICAN HEALTH ALLIANCE AND ITS COMMITMENT TO FURTHERING IMPROVEMENTS IN HEALTH FOR ALL.

MR. CHAIRMAN AND MEMBERS OF THE COMMITTEE, I AM STEADFASTLY IN SUPPORT OF YOUR MOVING THE NATION FORWARD IN HEALTH INFORMATION TECHNOLOGY AND WORKING TO ENSURE THAT THE HEALTH OF ALL POPULATIONS BENEFIT FROM THE IMPLEMENTATION OF THE PROVISIONS OUTLINED IN YOUR DISCUSSION DRAFT. WE CAN GO ANY PLACE IN THE WORLD AND USE OUR BANK CARD TO GET MONEY OUT OF OUR BANK ACCOUNT – BUT, WE CANNOT GO ACROSS THE STREET -- AND -- BE ABLE TO KNOW WHETHER A CHILD'S IMMUNIZATIONS ARE UP-TO-DATE. IN FACT, MOST BANK RECORDS, BILLS, PERSONAL COMMUNICATIONS, AND SECURITY EXCHANGES ARE MAINTAINED ELECTRONICALLY -- WHILE THE VAST

MAJORITY OF THE NATION'S HEALTH CARE ENTITIES ARE NOT USING ELECTRONIC HEALTH RECORDS TECHNOLOGY – ONLY ABOUT 18 PERCENT. THIS TELLS US SOMETHING ABOUT OUR HEALTH CARE SYSTEM.

I KNOW THAT YOU ALREADY KNOW THAT WE HAVE ABSOLUTELY THE BEST DOCTORS, BEST NURSES, BEST HOSPITALS, AND CUTTING EDGE RESEARCH IN THE WORLD. BUT, YOU ALSO KNOW THAT WE DO NOT HAVE THE BEST HEALTH CARE. IN FACT, WE HAVE A VERY EXCELLENT SICK-CARE SYSTEM. THE PROBLEM IS WE DO NOT HAVE A HEALTH CARE SYSTEM. HEALTH INFORMATION TECHNOLOGY WILL HELP SERVE AS THE CONNECTOR -- BRINGING TOGETHER MULTIPLE PIECES OF ALL OF THIS EXCELLENCE – TO BETTER SERVE THE PATIENT AND THEIR HEALTH CARE PROVIDERS ACROSS ALL SEGMENTS OF THE POPULATION.

I AM CONCERNED ABOUT ALL AMERICANS AND I AM CONFIDENT THAT IF I ADVOCATE FOR THE MOST MARGINALIZED OF THE AMERICAN PEOPLE THAT WE WILL SECURE HEALTH CARE OF EQUAL HIGH QUALITY FOR ALL. MEMBERS OF THIS IMPORTANT COMMITTEE HAVE THE OPPORTUNITY -- TO ALSO BE THE VOICE AND VISION FOR THE POOR AND POWERLESS. I URGE YOU TO USE YOUR TREMENDOUS POWERS -- AS I KNOW YOU CAN, AND AS IS REFLECTED IN THIS DISCUSSION DRAFT -- BY THE MULTIPLE SECTIONS THAT ADDRESS THE NEEDS OF ALL POPULATIONS. THIS IS CRITICAL AS MANY OF THE HEALTH CARE PROVIDERS THAT ARE SERVING THOSE MOST IN NEED

CANNOT AFFORD HEALTH INFORMATION TECHNOLOGIES. VULNERABLE POPULATIONS MUST NOT BE LEFT BEHIND, AND WE LOOK FORWARD TO WORKING WITH YOU IN THAT REGARD.

MR. CHAIRMAN AND MEMBERS OF THE SUBCOMMITTEE, I AM VERY ENCOURAGED BY AND APPRECIATE THE HARD WORK THAT CHAIRMEN DINGELL AND PALLONE, AND RANKING MEMBERS BARTON AND DEAL HAVE PUT INTO DEVELOPING THIS DISCUSSION DRAFT AND WE KNOW THAT IT WILL REQUIRE YOUR COLLECTIVE EFFORTS, WISDOM AND SUPPORT TO MOVE IT FORWARD.

WE ARE ENCOURAGED BY MANY COMPONENTS OF THE DRAFT – INCLUDING THE CODIFICATION OF THE OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH INFORMATION TECHNOLOGY. THIS IS KEY TO THE OVERALL EFFECTIVENESS OF THE NATION'S UTILIZATION OF HEALTH INFORMATION TECHNOLOGY.

WE ARE ENCOURAGED BY THE ESTABLISHMENT OF THE ADVISORY COMMITTEES WHICH WILL SUPPORT THIS EFFORT. – HOWEVER, TO HELP ENSURE THE FULL BENEFIT OF THE AMERICAN PEOPLE'S EXPERTISE IN THIS NATIONAL INVESTMENT IN HEALTH, MEMBERS OF THIS SUBCOMMITTEE MUST ENSURE DIVERSITY ON THESE COMMITTEES AND THROUGHOUT THIS HEALTH INFORMATION TECHNOLOGY ENTERPRISE – FROM DEVELOPMENT, TO

IMPLEMENTATION, TO MONITORING. DIRECT INCLUSION IS KEY. IN ADDITION, THE AGENCIES INVOLVED MUST INCLUDE THE OFFICE OF MINORITY HEALTH, OFFICE OF RURAL HEALTH, OFFICE FOR CIVIL RIGHTS AND OTHER KEY FEDERAL AGENCIES SUCH AS THE VA AND DoJ.

WE ARE ENCOURAGED BY THE DRAFT'S BIFURCATED APPROACH TO THE DEVELOPMENT OF STANDARDS USING BOTH A POLICY SETTING COMMITTEE AND A HEALTH INFORMATION TECHNOLOGY STANDARDS SETTING COMMITTEE; AND BY THE DRAFT'S ESTABLISHMENT OF A PROMINENT STANDARDS DEVELOPMENT ROLE FOR THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.

ALSO, WE FIND ENCOURAGING THE PROVISIONS ESTABLISHING A RESOURCE CENTER; GRANTS AND LOANS; EDUCATION AND RESEARCH; AND DE-IDENTIFIED INFORMATION WHICH CAN BE USED TO CAPTURE HEALTH DISPARITY METRICS. FOR THE OVERALL HEALTH BENEFIT OF THE NATION'S DIVERSE POPULATIONS, WE MUST ENSURE THAT DATA IS CAPTURED ACROSS EACH COMMUNITY TO ALLOW FOR THE AGGREGATING AND DISAGGREGATING OF DATA FOR ANALYSES OF TREATMENT EFFECTIVENESS AND OTHER HEALTH BENEFICIAL INQUIRIES. DOING SO CAN ULTIMATELY ASSIST OUR NATION IN HEALTH CARE COST SAVINGS -- BY BETTER ENABLING PREVENTION AND TREATMENT STRATEGIES.

WE ARE ENCOURAGED BY PROVISIONS WHICH CALL ON THE NATIONAL COORDINATOR TO ASSESS AND PUBLISH THE IMPACT OF HEALTH INFORMATION TECHNOLOGY ON COMMUNITIES WITH HEALTH DISPARITIES. HOWEVER, TO BE EFFECTIVE, SUCH ASSESSMENT MUST BE ONGOING. THIS WILL DO MUCH TO PROMOTE ITS WIDE SPREAD ADOPTION AND UTILIZATION. WE ALSO BELIEVE THAT THROUGH APPROPRIATE USE OF STANDARDS, HEALTH DISPARITIES CAN BE IDENTIFIED AND ADDRESSED. LIKEWISE, THE PRIVACY PROVISION STANDARDS MUST BE CONTINUALLY MONITORED AND REPORTED ON. PATIENTS AND CONSUMERS MUST BE ENGAGED AND INFORMED OF THE EVOLVING PRIVACY PROCESS THAT PROTECTS THEIR HEALTH INFORMATION AND TRUST ITS EVOLUTION. USING HIPAA AS A BASELINE HELPS TO MOVE US FORWARD MORE EFFECTIVELY.

WITH RESPECT TO HEALTH DISPARATE COMMUNITIES, AMONG THE COMMON THREADS ACROSS THEM ARE GAPS IN CARE, LACK OF ACCESS, INCREASED MORTALITY AND MORBIDITY, BIAS IN DELIVERY OF HEALTH CARE, LANGUAGE BARRIERS, VOIDS IN DATA, CULTURAL DIFFERENCES, NEED FOR CULTURAL COMPETENCY, THE LIST GOES ON AND YES, RACE DOES MATTER. AS THE INSTITUTE OF MEDICINE'S UNEQUAL TREATMENT STUDY VIVIDLY REVEALED, MINORITIES RECEIVE A LESSER QUALITY OF CARE THAN THEIR WHITE COUNTERPARTS EVEN WHEN DATA IS ADJUSTED FOR EDUCATION, SOCIO-ECONOMIC STATUS, ACCESS TO CARE, COVERAGE, AND OTHER KEY FACTORS. THE APPLICATION OF HEALTH INFORMATION

TECHNOLOGY CAN HELP TO LEVEL THE PLAYING FIELD -- AS STANDARDS OF CARE AND TREATMENT GUIDELINES ARE INCORPORATED INTO THE PATIENT'S ELECTRONIC HEALTH RECORD -- AIDING CLINICAL DECISION MAKING AND HOPEFULLY REMOVING UNINTENTIONAL BIAS.

THE CARE AND TREATMENT, DISEASE PREVENTION, AND HEALTH PROMOTION IS MORE CHALLENGING FOR THOSE THAT ARE: UNINSURED; UNDERINSURED; THOSE FORCED TO USE EMERGENCY ROOMS AS THEIR PRIMARY CARE PROVIDER; THOSE THAT ARE DISPLACED BY DISASTER SUCH AS KATRINA AND RITA; AND THOSE WITH NO MEDICAL HOME. -- EACH CAN BENEFIT BY UTILIZATION OF HEALTH INFORMATION TECHNOLOGY. HAVING THEIR HEALTH INFORMATION MAINTAINED INTACT AND PORTABLE, THIS BENEFITS THE PATIENT AND HEALTH CARE PROVIDERS.

IN ADDITION, HEALTH INFORMATION TECHNOLOGY HELPS TO ENSURE CONSISTENCY IN CARE, MORE LIKELY APPLICATION OF MEDICAL ADVANCES, REDUCTION OF REDUNDANT AND DUPLICATIVE MEDICAL WORK-UPS AND TESTS; OVERALL, IT HELPS TO PROVIDE A MORE STABLE, MORE EFFECTIVE, MORE RESPONSIVE AND SAFER HEALTH CARE ENVIRONMENT. HEALTH INFORMATION TECHNOLOGY SPECIFICALLY APPLIED TO CAPITALIZE ON THESE BENEFITS WILL DO MUCH TO IMPROVE OUR NATION'S GLOBAL HEALTH STANDING. IN FACT, RESEARCH HAS WELL ESTABLISHED THAT ADDRESSING HEALTH DISPARITIES WILL REQUIRE MULTIPLE STRATEGIES, A MULTI-

DISCIPLINARY APPROACH AND MULTIFACETED TOOLS. THE APPLICATION OF HEALTH INFORMATION TECHNOLOGY IS A KEY TOOL IN THAT PORTFOLIO.

IN CLOSING, MR. CHAIRMAN AND MEMBERS OF THIS ESTEEMED COMMITTEE, WE MUST HAVE THE WILL TO CHANGE – WE HAVE THE TOOLS! LET'S CONTINUE TO WORK FORWARD -- TOGETHER -- IN ADDRESSING OUR NATION'S PRESSING HEALTH ISSUES. TO QUOTE DR. KING, *"OF ALL THE FORMS OF INEQUALITY, INJUSTICE IN HEALTH CARE IS THE MOST SHOCKING AND INHUMANE. ...* WE LOOK FORWARD TO WORKING WITH YOU ON THIS IMPORTANT DISCUSSION DRAFT. THANK YOU FOR THIS OPPORTUNITY. I LOOK FORWARD TO ANSWERING ANY QUESTIONS THAT YOU MAY HAVE.

Mr. PALLONE. Dr. Peel.

STATEMENT OF DEBORAH C. PEEL, M.D., FOUNDER AND CHAIR, PATIENT PRIVACY RIGHTS

Dr. PEEL. Thank you for the opportunity to testify today on the health information technology and privacy draft. I applaud everyone's hard work on this bill.

I am Dr. Deborah Peel, and I am the founder and Chair of Patient Privacy Rights. We have 5,000 members. We educate consumers. We champion smart policies. And we are holding industry accountable to protect your health information.

We also lead the coalition, the bipartisan coalition for patient privacy, and we represent over 7 million Americans' interests. I am known for being really passionate about privacy. My patients taught me about privacy. I know that you cannot have effective treatment unless patients trust that their physicians will be able to keep their sensitive information private.

People came to me, starting 30 years ago, and paid cash because they had lost a job or their reputation had been harmed when someone saw their information that should not have. At Patient Privacy Rights we hear every day from people in every State, desperate for help.

People have found their health records on the Internet. Veterans are afraid to get treatment for post-traumatic stress disorder, and people complain to us because employers want them to turn over access to their health records as a condition of getting employment. So while I may be passionate about this issue, the idea that your most embarrassing, sensitive health conditions should stay private and that you should control that information is not radical. In fact, it is conservative.

Today, everybody wants access to health information—employers, insurers, law enforcement—but I am here to tell you, electronic records systems create a real risk for patient privacy. My patients will tell you, the existing laws do not protect them. Four million people, 4 million providers and their employees today decide when, where, and who sees your health information technology. Not you.

Today, electronic systems aren't secure. Employers and insurers use this information to decide if you get jobs or coverage. Just one prescription data miner in 2006 made $2 billion—that is B, billion dollars. A national insurer aggregates themselves the data of 79 million Americans, and every prescription in this Nation is sold and data mined every day. It doesn't matter if you pay cash.

Americans need you, all of you, to ensure progress with privacy in this bill. But, first, we have to have a definition of privacy. We don't even have one. We are not even talking on the same page about what that means. We lack the NCVHS IOM definition that health information privacy is the individual's right to control the acquisition, uses and disclosures of identifiable information; or go back to Hippocrates, "Whatsoever I shall see or hear of the lives of men and women not fitting to be spoken, I will keep inviolably secret."

Or in 1974, HEW, the Department of Health, Education and Welfare, developed the Code of Fair Information Practices. This is their definition: "There must be a way for a person to prevent informa-

tion about them obtained for one purpose, being used for other purposes without consent." Privacy means control over information. If you don't control your information, you don't have privacy.

Congress needs to adopt a definition of health privacy. Please. You choose. Choose a definition. Let's start from one place.

Second, we have got to restore Americans' abilities to control their personal health information. Codify what everyone assumes happens when they see a doctor, when they go to see a doctor. They assume that what they say in a doctor's office stays in the doctor's office. Ladies and gentlemen, getting your consent before anyone discloses your diagnosis of cancer, heart disease, diabetes—you name it, depression—is not radical. In fact, today, obtaining consent is very easy using smart technology.

To accept the argument that consent is a burden or impractical means we accept that it is OK for industry not to even try and communicate with their customers. It is OK for those who have everything to gain to decide how your information is used. Well, that is not OK with us. Destroying the bond of trust between physicians and patients has worked for millennia—millennia. That is what is radical in this debate.

Finally, do not delegate the power to change Americans' longstanding right to privacy from others. Three-quarters of Americans want government, not industry, to set the rules and privacy protections they will have. Two-thirds want government, not industry, to set the rules regarding secondary uses of information.

The lack of privacy is harmful and it is deadly. According to HHS, 2 million people with mental illness don't get treatment because of privacy; 600,000 people with cancer are afraid to get early diagnosis and treatment because of privacy. This is from HHS that says that. One in eight Americans does something to put their health at risk because of privacy. They either see different doctors, they ask them to change diagnoses, they are afraid of taking tests.

Mr. PALLONE. Dr. Peel, I am sorry, but you are 1 minute over; if you could, please summarize.

Dr. PEEL. Let me just stop and say—I just want to say one other thing. I have been face to face with my patients over 30 years and I have seen how their lives are damaged and harmed when information gets in the wrong hands. But I can't even tell you their stories because I took an oath. And if I break that oath and violate their trust, then I can't help them.

Now is your opportunity; it is your opportunity to define privacy and make it a reality again for all Americans. I am really grateful for this opportunity to talk with you and to work with you on improving this bill and protecting Americans. I would ask you to please take the same oath that I do and protect Americans' trust in the health care system.

Thank you so much.

Mr. PALLONE. OK. Thank you.

[The prepared statement of Dr. Peel follows:]

Written Testimony
Deborah C. Peel, MD, Founder & Chair, Patient Privacy Rights

Thank you for the opportunity to testify today on the discussion draft of "Health Information Technology and Privacy Legislation." I applaud the hard work of this committee and its staff.

My name is Dr. Deborah Peel. I am the founder and chair of Patient Privacy Rights, a national organization that educates consumers about the importance of health privacy, champions smart policies and technologies, and holds industry accountable to protect what's most valuable—our health, our families and our reputation. We also lead the bipartisan Coalition for Patient Privacy, representing over seven million Americans.

It is fairly well known that I am passionate - to say the least - about privacy. And the reason for that is that I learned about privacy from my patients. As a practicing physician in the field of psychiatry I know that effective treatment depends upon the trust established between a doctor and a patient. When I first entered practice, people came and paid me cash on the barrelhead because they had lost jobs or their reputations were ruined when someone saw their health records that should not have. I have spent thirty years hearing from people whose privacy was violated.

So while I may be passionate, this idea that your most embarrassing conditions should stay private, or that information about YOU should be in your control, is not a radical concept.

P.O. Box 248 • Austin TX 78767 • 512.732.0033
www.patientprivacyrights.org

In an era when records were kept in manila folders in locked file cabinets, it was not difficult to ensure medical records were private. But we are in a different world today. Today employers, insurers, even law enforcement want access to health records, and with much of this information moving to electronic formats, the risk to patient privacy is very real. **My patients will tell you: existing laws don't go far enough nor do enough.** You'll hear the same from more than 1.3 million Americans this year alone who had their information breached, not to mention another 1,000 of our veterans cared for by Walter Reed Army Medical Center.

Despite the fact that HIPAA requires more stringent privacy-protective state laws and medical ethics to prevail over the privacy 'floor' in HIPAA, the opposite has occurred. HIPAA regulations allowing broad access to personal health information without consent have been widely used as the nation's privacy standard. Data mining and sale of health information is rampant. This was not the intent of Congress.

Privacy in electronic health systems is threatened in three ways:

1) Individuals have no control over the use or disclosure of personal health information in electronic systems. That means 4 million providers and their employees decide when, where, and who gets your sensitive data, not you.

2) Electronic systems are not secure. A Presidential Cybersecurity Task Force found that attacks on electronic information systems are growing by 20% a year[1], and the Office of Management and Budget found that attacks on federal electronic information systems grew 60% between 2006 and 2007.[2]

3) Health data is it is extremely valuable. Americans' personal health information is worth billions.

---

[1] "Cyber Security: A Crisis in Prioritization," President's Information Technology Committee, p. 5 (Feb. 28, 2005)
[2] "Feds Losing War On Information Security, Senators Told," Govexec.com (March 13, 2008) http://www.govexec.com/story_page.cfm?articleid=39518&dcn=e_gvet

- Employers and insurers access personal health data to make decisions about employment and coverage.
- In 2006, one prescription data miner reported revenues of $2 billion dollars.
- In 2006, a national insurer with plans in all 50 states started a business unit that aggregates and sells the data of 79 million enrollees.
- Every prescription in the U.S. is data mined and sold, even if you pay cash.

How do we address these threats? How do we have both progress and privacy?

First, go back to basics. Define privacy. The "P" in HIPAA does not stand for privacy. NCVHS defined health information privacy as "an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data." Without a definition of privacy, we cannot even agree on what needs to be fixed. Here are a few other accepted definitions:

- The *Hippocratic Oath* says "Whatsoever I shall see or hear of the lives of men or women which is not fitting to be spoken, I will keep inviolably secret."
- The *Code of Fair Information Practices 1974* says "There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent."

They all say the same thing: privacy means control over personal information—if you have no control, you have no privacy.

HHS still has not defined privacy. HHS recently spent $500,000.00 on a project to develop definitions for electronic health systems. They defined RHIOs, they defined HIEs, they defined lots of things, but they still have not defined privacy.

When privacy is defined, the right to health privacy must be confirmed in statute. Congress must adopt a definition, Congress choose one.

Second, restore Americans' control over their personal health information. At a minimum, any health IT legislation must codify what Americans assume happens when they visit

their doctors: that what they "say in the doctor's office stays in the doctor's office," and that it is not be shared in any way with others without their permission.

Ladies and Gentleman, getting consent, or permission, to disclose your diagnosis of cancer, an STD, a Paxil prescription or even having the flu is not radical. In fact, obtaining consent is easier than ever with health IT. To accept the argument that consent is too burdensome or impractical means we accept that –

~It is O.K. for the health industry to not even *try* to communicate with their customers, the patients, and

~It is O.K. to just let those who have the most to gain and nothing to lose decide how personal information is used.

Well, that is not O.K. What is radical is to destroy the bond of privacy and trust between physicians and patients that has worked for millennia.

In addition to these fundamental additions to the current HITEC draft we ask that you significantly strengthen public participation in this bill. The proposed members of the HIT Policy and Standards Committees are dominated by conflicted appointees from the health industry; their recommendations will reflect their interests. These committees must include sufficient representation by those without ties to government or the private sector, including consumer advocates, privacy experts, scholars, and those with expertise in medical ethics. We offer a number of suggestions in our detailed comments.

Congress must not delegate the power to alter or eliminate Americans' long-standing rights to health information privacy. Americans clearly want Congress to act to keep their health records private.

- The Markle Foundation Survey found that ¾ of the public want the government to set rules to protect the privacy and confidentiality of electronic health information, and

- Two-thirds want the government to set rules controlling the secondary uses of information.
- Federal Computer Week found that 66% of Americans believe Congress should make protecting information systems and networks a higher priority.[3]

The lack of privacy is both harmful and deadly. Millions of Americans avoid doctors and delay care for fear their employer will find out, their insurer will drop them or a vast world of strangers will know their most intimate details.

- According to HHS, **two million** Americans with mental illness do not seek treatment for this reason.[4]
- **600,000** cancer victims do not seek early diagnosis and treatment.[5]
- **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).[6]
- The California Health Care 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 - Avoiding tests altogether.*[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]

The lack of privacy contributes to the highest suicide rate among active duty soldiers in nearly 30 years. CBS News reports an average of 18 veterans commit suicide every day. Soldiers

---

[3] Federal Computer Week, May 23, 2006
[4] 65 Fed. Reg. at 82,779
[5] 65 Fed. Reg. at 82,777
[6] 65 Fed. Reg. at 82,778
[7] CHCH Consumer Health Privacy Survey, June 2005
[8] "Invisible Wounds of War", The RAND Corp., p. 436 (2008)

know their treatment and records are not private. This is unacceptable statistic for our men and women in uniform.

To build a system people trust, we need a definition of privacy, and we need to restore the right to health privacy. Millions will not agree to treatment without the guarantee their health records will be private.

I've been sitting face to face with patients for over thirty years. It is that human contact that makes me so passionate about privacy. Frankly, it is heart breaking to see the real destruction caused when private, intimate information gets in the wrong hands. Patient Privacy Rights, in operation for just a few years, hears daily from patients from every state in this nation, desperate for help and looking for justice.

We will always have nosy neighbors. We will always have security breaches at some level, regardless of the security standards we implement. The one thing you can do and must do is minimize what happens to our private information on a daily basis.

I am very grateful for your time and this opportunity to come before you. We respectfully submit our written, detailed comments for this draft legislation as well.

patientprivacyrights

Brief Summary
Testimony by Deborah C. Peel, MD,
Founder & Chair of Patient Privacy Rights

As a practicing physician in the field of psychiatry for over thirty years, I know that effective treatment depends upon the trust established between a doctor and a patient. *The idea that your most embarrassing conditions should stay private, or that information about YOU should be in your control, is not a radical concept.*

Despite the fact that HIPAA requires more stringent privacy-protective state laws and medical ethics to prevail over the privacy 'floor' in HIPAA, the opposite has occurred. Today:

1) Individuals have no control over their personal health information.
2) Electronic systems are not secure.
3) Americans' health data is worth billions.

How do we address these threats? How do we progress with privacy?

First, define privacy. NCVHS defined health information privacy as "an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data." Privacy means control over personal information—if you have no control, you have no privacy.

Second, restore Americans' control over their personal health information. At a minimum, any health IT legislation must codify in law what Americans assume happens when they visit their doctors: that what they "say in the doctor's office stays in the doctor's office."

Third, strengthen public participation significantly in this bill. The proposed members of the HIT Policy and Standards Committees are dominated by conflicted appointees from the health industry; their recommendations will reflect their interests. These committees must include sufficient representation by those without ties to government or the private sector, including consumer advocates, privacy experts, scholars, and those with expertise in medical ethics.

I've been sitting face to face with patients for over thirty years. It is frankly heart breaking to see the real destruction caused when private, intimate information gets in the wrong hands. Patient Privacy Rights, in operation for just a few years, hears daily from patients from every state in this nation, desperate for help and looking for justice.

We will always have nosy neighbors. And we will always have security breaches at some level, regardless of the security standards we implement. The one thing you can do and must do is minimize what happens to our private information on a daily basis. Thank you.

P.O. Box 248 • Austin TX 78767 • 512.732.0033
www.patientprivacyrights.org

Mr. PALLONE. Ms. McGraw.

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

Ms. MCGRAW. Thank you very much, Mr. Chairman. I also want to thank you for the opportunity to testify here today and also to thank you, Ranking Member Deal, as well as Chairman Dingell and Ranking Member Barton and their staffs for the hard work that they put in on this bill.

I am the Director of the Health Privacy Project at CDT, the Center for Democracy and Technology. CDT has a long history of expertise on Internet and information privacy issues. The Health Privacy Project has a decade of experience in advocating for privacy and security of health information, and so those two organizations have recently merged together in order to come with up with workable solutions to better protect the privacy and security of health information online.

CDT supports efforts to expand the adoption of health information technology and health information exchange electronically, but we won't realize these benefits until we build in the right privacy and security protections. I think others here have testified very well that, in fact, people will fear having their information be part of the systems if we can't assure them that we have taken the right steps to protect their privacy and security.

This technology actually has the tools to be better protective than paper, if we make people use it; but we also know that if we don't, the fact that this information is flowing more freely out there electronically, in fact, does magnify the risk. A box of paper records that gets stolen has one set of consequences. Information that is inadvertently put up online or was stolen from a laptop has consequences for tens of thousands or even hundreds of thousands of people instantly. We can do better.

To really build public trust in these systems, what we need is a comprehensive privacy and security framework that is based on fair information practices, which is typically what we look to when we want to protect personal health information and we don't have to start from scratch. The HIPAA privacy and security rules provide a comprehensive framework, but there are gaps in HIPAA; and we need to build on it and fill those gaps for entities in the health care system and consider the fact that in this new environment health information is migrating outside of the traditional health care system and is being handled by companies that aren't traditional health care players and might be operating on a different business model.

This draft bill begins the work of developing that comprehensive framework, and we are proud to support it. So we really are calling on Congress to think big and to have a comprehensive vision, but we know these topics are quite complex. It is not easy to think about the right privacy and security protections to put in place when we also need to consider that we want information to flow for legitimate purposes.

So we are advocating for incremental implementation, which is one of the reasons why we like this bill. It takes critical steps to-

ward the goal of a comprehensive framework by establishing incremental, workable privacy and security solutions that build on current law and target many of the new issues that are raised in this new environment.

It doesn't do everything in this draft. I think we are going to need to continue to revisit this over time, build on the foundation we created in HIPAA and that, hopefully, will be built on with this bill; and as the systems evolve, continue to pay attention to this. But the discussion draft breaks the private logjam and allows us to move the conversation forward to the next level, which is really what we need to do.

We support the provisions in the bill. I will highlight just a few of them. We like that it clarifies that the businesses' associates should be directly accountable for complying with the security rules and for the provisions of their contracts with respect to how they are able to use information.

We like the breach notification provisions, although we do ask the committee to consider strengthening the incentives to use protective technologies like encryption by providing possibly a safe-harbor, rebuttable presumption when the data is encrypted that there isn't a need to notify unless for some reason you have information that the data encryption isn't working; clarification of the marketing rule, tasking HHS and the FTC to develop recommendations for privacy and security protections and breach notifications for these new entities; PHRs, particularly where we think they are offered by companies outside of the health care system, whether it is employers or traditional Internet-based companies. Extending HIPAA to cover those would not work; HIPAA's framework works for health care system entities, but it would have unintended consequences if grafted on top of this industry, which again works under a different business model.

We also hope the committee will give some further consideration to enforcement of HIPAA either in this bill or subsequently down the road. I know Congressman Waxman mentioned earlier that there hasn't been a single civil monetary penalty that has been levied. We also know that the Department of Justice has been hamstrung somewhat by an internal memo that suggests that you can't get to employees of covered entities for criminal violations. I am happy to go into that in more detail, but we hope the committee will look into those issues further.

Again, I thank you for your very hard work on this bill. We support it, and I am happy to answer any questions that you might have.

Mr. PALLONE. Thank you, Ms. McGraw.

[The prepared statement of Ms. McGraw follows:]

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

Statement of Deven McGraw

Director, Health Privacy Project

Center for Democracy & Technology

Before the

House Energy and Commerce Committee

on the

Discussion Draft of Health Information Technology and Privacy Legislation

June 4, 2008

Chairman Dingell, Ranking Member Barton, and members of the Committee, thank you for holding this hearing on the discussion draft of Health Information Technology and Privacy Legislation developed by the Chairman and Ranking Member of the Committee, and Chairman Pallone and Ranking Member Deal of the Subcommittee on Health.

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 earlier this year to take advantage of CDT's long history of expertise on Internet and information privacy issues and to come up with workable solutions to better protect the privacy and security of health information on-line and build consumer trust in e-health systems.

Just a couple of weeks ago, CDT released a comprehensive paper calling on Congress to enact – and all stakeholders to adopt - a comprehensive privacy and security framework to cover electronic health information. Some of the points raised in that paper are highlighted in this testimony today, but I also request that the full copy, which is attached and can be found at www.cdt.org/healthprivacy/20080514Hpframe.pdf, be entered into the hearing record.

The discussion draft takes critical steps toward that goal by setting forth incremental, workable privacy and security solutions that build on current law and target many of the key issues raised by the new e-health environment. CDT is pleased to support this draft, which will help increase public trust in health information technology and health information exchange and facilitate the movement of the nation to an interconnected, electronic health system.

Privacy and Security Protections are Critical to Health IT

Health information technology (health IT) and health information exchange can help improve health care quality and efficiency, while also empowering consumers to play a greater role in their own care. 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 – because they believe such access is likely to increase their quality of care. At the same time, people have significant concerns about the privacy of their medical records. In a national survey conducted in 2005, 67% of respondents were "somewhat" or "very concerned" about the privacy of their personal medical records.[1] 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. [2]

[1] National Consumer Health Privacy Survey 2005, California HealthCare Foundation (November 2005) (2005 National Consumer Survey).

[2] Study by Lake Research Partners and American Viewpoint, conducted by the Markle Foundation (November 2006) (2006 Markle Foundation Survey).

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 for appropriate purposes without needing to create large, centralized databases that can be vulnerable to security breaches. Encryption can help ensure that sensitive data is not accessed when a system has been 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.[3]

At the same time, the computerization of personal health information—in the absence of strong privacy and security safeguards—magnifies the risk to privacy. As the recent spate of large-scale privacy and security breaches demonstrates, serious vulnerabilities exist now. Tens of thousands of health records can be accessed or disclosed through a single breach. Recent headlines about the theft of an NIH laptop loaded with identifiable information about clinical research subjects underscore these concerns, and this is 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

[3] See For The Record: Protecting Electronic Health Information, Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure, Computer Science and Telecommunications Board, National Research Council (National Academy Press, Washington, DC 1997) for a discussion of the inability of systems to be 100% tamperproof.

privacy rules by federal authorities, deepens consumer distrust in the ability of electronic health information systems to provide adequate privacy and security protections.[4]

With rare exception, national efforts to advance greater use of health IT have not adequately or appropriately addressed the privacy and security issues raised by the movement to electronic health 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.

Protecting privacy is important not just to avoid harm, but because good health care depends on accurate and reliable information.[5] 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.[6] 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 disclosed.[7] 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

[4] See http://www.cdt.org/healthprivacy/20080311stories.pdf for stories of health privacy breaches and inappropriate uses of personal health information.

[5] 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).

[6] Protecting Privacy; Promoting Health/Protecting Privacy; 2005 National Consumer Survey.

[7] Harris Interactive Poll #27, March 2007.

their personal medical records and are more likely than average to practice privacy-protective behaviors.[8]

The consequences of this climate of fear are significant – for the individual, for the medical community, and for public health:

- The quality of care these patients receive may suffer;
- Their health care providers' ability to diagnose and treat them accurately may be impaired;
- The cost of care escalates as conditions are treated at a more advanced stage and in some cases may spread to others; and
- Research, public health, and quality initiatives may be undermined, as the data in patient medical records is incomplete or inaccurate.[9]

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 than building it at the start. Now—in the early stages of health IT adoption—is the critical window for addressing privacy.

---

[8] 2005 National Consumer Survey.

[9] Id.

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 a comprehensive privacy and security framework that sets clear parameters for access, use and disclosure of personal health information for all entities engaged in e-health. 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, most notably the HIPAA Privacy Regulation, which established the first federal health privacy framework.[10] While there is no single formulation of the "FIPs," the Common Framework developed by the Markle Foundation's multi-stakeholder Connecting for Health initiative, would:

- Implement core privacy principles;
- Adopt trusted network design characteristics; and
- Establish oversight and accountability mechanisms.[11]

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. The framework should be implemented in part by strengthening the HIPAA Privacy Rule for

[10] Other potential sources for policy recommendations include the GAO, the National Center for Vital Health Statistics and the National Governor's Association State Alliance for eHealth.

[11] See www.connectingforhealth.org for a more detailed description of the Common Framework.

records kept by the traditional health system participants, but also needs to address the increased migration of personal health information out of the traditional medical system.

As set forth in more detail below, we are pleased that this discussion draft addresses so many of the elements of fair information practices. The draft takes some critical steps forward in the effort to establish a framework of comprehensive privacy and security protections that will build consumer trust in health IT and help break the privacy "logjam" that has to date thwarted efforts to increase the federal investment in building an interoperable, nationwide electronic health system. We hope that this draft marks the beginning of a longer-term effort on the part of Congress and other policymakers to address privacy and security of health information as part of an overall conversation about how to move our health care system into the 21st Century.

Strengthening HIPAA Privacy and Security Rules to Meet New Challenges

The federal privacy and security rules that took effect in 2003 under the Health Insurance Portability and Accountability Act (HIPAA) reflect elements of a comprehensive framework and provide important privacy protections governing access, use and disclosure of personally identifiable health information by some entities in the health care system. 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. This discussion draft includes important provisions to address these gaps. For example:

- State and regional health information organizations or health information exchanges (also known as RHIOs or HIEs), which may aggregate and facilitate exchange of personal health information, are often not covered by the Privacy Rule. The discussion draft makes it clear that RHIOs, HIEs, E-prescribing Gateways must be business associates of covered entities in order to receive and exchange protected health information. The draft strengthens the protections for consumers whose information is maintained or accessed by business associates by making these entities directly accountable for meeting the HIPAA Security Rule Provisions and making them subject to the HIPAA civil or criminal penalties for failure to comply with those rules. The draft also makes it clear that business associates cannot access, use or disclose protected health information except in accordance with the provisions of their business associate contract and makes business associates directly accountable to federal authorities for any failure to comply with the data use provisions in these contracts. These provisions in the HIPAA regulations are fundamental tenets of good data stewardship, and anyone who touches this sensitive data should be accountable for complying with them.

- The discussion draft establishes a federal right to be notified in the event of breach by a covered entity or business associate of protected health information, if the unauthorized use of the information could reasonably result in substantial harm, embarrassment, inconvenience or unfairness to the individual. 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.

We ask the supporters of this discussion draft to consider establishing a rebuttable presumption that encrypted information that is inappropriately accessed or disclosed is not subject to the notification requirements, which is the approach followed in the draft with respect to breach notification requirements for personal health record vendors.[12] Such an approach would create a powerful incentive for entities that hold personal health information to adopt strong encryption controls, thereby significantly minimizing the likelihood of data breach and consumer harm.

- As noted above in our testimony, more than 3/4 of consumers are concerned that their medical information will be used to market products or services back to them. We hear frequently from people who have received communications encouraging them to use specific drugs or other health care products or services that they are alarmed that someone must have accessed their medical information in order to target them with these communications. The HIPAA Privacy Rule already prohibits the use of protected health information for marketing purposes without a patient's express authorization. But the definition of marketing has been interpreted by some to permit, without authorization, "patient education" communications that consumers would clearly perceive to be marketing. The discussion draft closes that loophole by making it clear that a communication

[12] In the alternative, the bill could establish that unauthorized access to or disclosure of unencrypted information is the "trigger" for breach notification, instead of leaving it up to the subjective judgment of the entity holding the information about whether the breach would harm or be embarrassing or unfair to the individual.

must meet all three of the exemptions in the current Privacy Rule marketing definition in order to be exempt from the requirement of patient authorization.

- 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 provide covered entities with the ability to easily track precisely who has accessed a patient's medical record, and we understand that most health care entities using electronic health records are already using these electronic "audit trails" to control who can access a patient's record and to track and monitor every touch of a patient's record. The discussion draft would require entities using these electronic tools to allow patients to receive a copy of that audit trail upon request. Few consumers are likely to take advantage of this right – but knowing it is possible to get a copy of who has accessed your medical records goes a long way to building consumer trust, and engages patients in the effort to ensure that information in their record is accurate, complete and current.

- The Privacy Rule gives patients the right to request a restriction on uses and disclosures of their information for treatment, payment and health care operations – but currently a covered entity is under no obligation to grant the request. The discussion draft makes it clear that in cases where a patient wants to pay for medical care out-of-pocket, a covered entity must honor a request to not disclose information related to that care to an insurer specifically for payment purposes.

We note that the draft still permits the covered entity to use and disclose information for treatment and health care operations, which includes a number of health care coverage functions that health insurers and plans have long claimed are critical to their business operations.

- A critical element of fair information practices is that data should be collected and used only for specific and appropriate purposes. 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 misinterpretation of the law. The discussion draft clarifies this provision – and further protects patient privacy – by making it clear that for uses other than treatment, covered entities should use a limited data set when they use and disclose protected health information for routine purposes, except in cases where a limited data set would not accomplish the legitimate purpose for which the information is sought.

Establishing Privacy Protections for Personal Health Records

Personal health records 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 offeror'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.[13] 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.

We believe the discussion draft – 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,

---

[13] 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.

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 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. We are pleased that the discussion draft lays the foundation for the establishment of these rules, and tasks the FTC with enforcing breach notification provisions until these rules can be established.

Congress Should Also Consider Strengthening HIPAA Enforcement

When Congress in enacted HIPAA in 1996, they enacted civil and criminal penalties for failure to comply with the statute – and these penalties applied also to the subsequent privacy and security rules implemented years later. Unfortunately, the HIPAA rules have never been adequately enforced. The HHS Office for Civil Rights (OCR), charged with enforcing HIPAA, has not levied a single penalty against a HIPAA-covered entity in the nearly five years since the rules were implemented, even though that office has found numerous violations of the rules.[14] 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 these criminal provisions to just

[14] "Effectiveness of medical privacy law is questioned," Richard Alonso-Zaldivar, Los Angeles Times (April 9, 2008) http://www.latimes.com/business/la-na-privacy9apr09,0,5722394.story.

covered entities, which has required prosecutors to bootstrap other legal provisions in order to criminally prosecute certain employees of covered entities who have criminally accessed, used or disclosed a patient's protected health information.[15]

The discussion draft requires HHS to annually report to Congress on enforcement of the HIPAA rules and establishes privacy officers in each HHS regional office, which are good first steps in securing better enforcement by both increasing Congressional scrutiny and raising the visibility of privacy as an HHS priority. But Congress should consider doing more, by either strengthening the provisions of the discussion draft as discussed below, or holding hearings on better enforcement of HIPAA and addressing the issue in subsequent legislation. A lax enforcement environment sends a message to entities that access, use and disclose protected health information that they don't have to 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.

Congress should:

- Carefully examine the statutory enforcement provisions in HIPAA and consider whether amendments are needed to strengthen OCR and DOJ's authority to impose criminal or civil penalties (and at a minimum, making it clear that the penalties can be assessed against covered entities, business associates, *and their employees* for violations of HIPAA).
- Consider how individuals who are significantly harmed by misuse of their

[15] See http://www.americanprogress.org/issues/2005/06/b743281.html for more information on the OLC memo and the consequences.

information can be made whole, or at least have access to meaningful recourse.

- Consider expressly authorizing state authorities (such as the attorneys general) to also enforce HIPAA.
- Consider establishing penalties for the re-identification of de-identified data.

Other Good Provisions of the Discussion Draft

- While the Privacy Rule includes criteria for de-identifying data, these criteria are now five years old – and new technologies and the increased availability of data on-line may be making it much easier to re-identify once de-identified health information. We are pleased that the discussion draft 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.

- We praise the discussion draft for authorizing $10 million for a comprehensive national education initiative to enhance public transparency regarding uses of health information and the effects of such uses.

- We also endorse the provisions calling for a GAO report on best practices related to disclosure among health care providers of protected health information for treatment purposes, as well as those that make it clear that stronger state privacy rules are preserved, which has always been an important component of HIPAA.

- We also believe the discussion draft sets up an administrative infrastructure for moving health IT forward that is better than what exists currently (or has been

proposed by the administration), and what is currently being considered in the Senate. In the draft, the Office of the National Coordinator (ONC) is firmly established in statute and specifically tasked to develop and execute a strategic health IT plan, with specific objectives, milestones, and metrics for facilitating electronic health records and health information exchange, including the incorporation of privacy considerations and security protections. ONC also must specify a framework for coordination and flow of recommendations and policies among the various administrative agencies involved in health IT, as well as the two federal advisory bodies established in the discussion draft. The draft establishes a Policy Committee, which must be accountable to the public and recommend a policy framework for the development and adoption of health IT, and any recommendations for technology standards must flow from these policy recommendations, which is the appropriate way to make policy governing health IT and health information exchange.

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.[16] A

[16] 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.

number of states have passed laws requiring patient authorization to access, use and disclose certain sensitive categories of health information, and federal law prohibits the disclosure of substance abuse treatment records without express patient authorization. HIPAA Privacy Rules currently prohibit the use of certain types of information, such as psychotherapy notes, or prohibit use of information for certain purposes, such as marketing, without express patient authorization, and the Rules provide individuals with the right to object to certain uses and disclosures (such as in facility directories or to family members). The discussion draft provides consumers with a right to restrict the disclosure of their health information to insurers for payment purposes where they are paying out-of-pocket for a health care product or service. Health information systems must be structured in a way that allows these consents to 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 <u>less</u> protective of privacy and confidentiality.

Among other reasons, a consent-based system places most of the burden of privacy protection on patients at a time where they may be least able to make complicated

decisions about use of their health data. Most don't read the details of a consent form and those that do often do not understand the terms. Many wrongly assume that the existence of a "privacy policy" means that their personal information will not be shared, even when the policy and the accompanying consent form say just the opposite.[17] If mere patient authorization is all that is needed to share data with third parties, highly sensitive patient information will be disclosed to entities that are completely outside the scope of the HIPAA privacy regulation. If consent becomes the focus of privacy protection, it is clear that patients will be exposed to unregulated and potentially uncontemplated uses—and misuses—of their data. Further, if reliance on consent by an individual for any particular use of his or her information is treated by policymakers as the key to privacy protection, the healthcare industry will have fewer incentives to design systems with stronger privacy and security protections.[18]

The discussion draft provides better protections for consumer's health information by addressing who can access, use, and disclose protected health information and for what purposes, and ensuring that these rules are applicable to and can be enforced against both covered entities and business associates; by providing for notification in the event of

---

[17] See "Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware" (with Nathan Good, Rachna Dhamija, Jens Grossklags, Steven Aronovitz, David Thaw and Joseph Konstan), presented at the 2005 Symposium on Usable Privacy and Security (SOUPS), also in ACM INTERNATIONAL CONFERENCE PROCEEDING SERIES; VOL. 93, PROCEEDINGS OF THE 2005 SYMPOSIUM ON USABLE PRIVACY AND SECURITY, Pittsburgh, Pennsylvania (2005); 2005 National Consumer Survey; " Research report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace," Joseph Turow. Deidre K. Mulligan & Chris Jay Hoofnagle, Survey conducted by University of Pennsylvania Annenberg School for Communications and UC-Berkeley Law School's Samuleson Law, Technology and Public Policy Clinic 2007.

[18] By contrast, a comprehensive approach puts the principal burden on the entities holding personal health information to protect privacy by placing clear enforceable limits on the collection and use of personal health information and backs it up with strong enforcement. See Beyond Consumer Consent: Why we need a Comprehensive Approach to Privacy in a Networked World, http://www.cdt.org/healthprivacy/20080221consentbrief.pdf.

breach; by requiring entities using electronic health records to provide consumers with an audit trail upon request; by giving consumers a right to restrict use of their data for payment purposes when they choose to pay out of pocket; by placing parameters around minimum necessary and making it clear that a limited data set should be used unless more identifiable information is legitimately needed; by tasking HHS and FTC to come up with recommendations for appropriate rules to protect consumers using PHRs; and by calling for an assessment by HHS regarding the criteria for deidentification of data need to be updated.

Conclusion

Thank you for the opportunity to present this testimony in support of the discussion draft, which we believe moves us significantly 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.

Attachment

Summary – Testimony of Deven McGraw, Center for Democracy & Technology
Hearing on Discussion Draft of Health IT and Privacy Legislation

- Health information technology (health IT) and health information exchange can improve health care quality and efficiency. But consumers have concerns about the privacy of their medical information on-line. Health IT has greater capacity to protect privacy – but the movement of health information on-line also magnifies the risks.

- The failure to address these risks deepens consumer distrust in e-health systems. Enhanced privacy and security built into health IT systems will bolster consumer trust and confidence and spur more rapid adoption of health IT.

- We need a comprehensive privacy and security framework that is based on fair information practices (i.e., the Markle Foundation Common Framework) and sets clear guidelines for use and disclosure of electronic health information. The framework should build on HIPAA and incorporate protections for health information held by non-health care entities.

- CDT supports the discussion draft, which takes critical steps toward establishing this comprehensive framework. In particular, CDT supports:
  - Clarifying that health information exchanges are business associates, and making business associates directly accountable for complying with the HIPAA Security Rules and the data use requirements in their business associate contracts;
  - Establishing a right of consumers to be notified in the event of a breach (CDT asks the Committee to consider creating a rebuttable presumption that notification is not necessary if the data that is breached is encrypted);
  - Clarifying the definition of marketing in the HIPAA Privacy Rule;
  - Giving patients the right to receive an audit trail from entities using electronic health records;
  - Granting patients the right to restrict disclosure of their information for payment purposes when they are paying out-of-pocket;
  - Requiring the use of a limited data set for non-treatment purposes, except when doing so would not be feasible.
  - Tasking HHS and FTC with coming up with recommendations for privacy protections for consumers using PHRs, and tasking FTC with enforcing breach notification provisions in the interim.
  - Requiring HHS to come up with guidance on de-identification.

- The Committee should consider doing more – either in this draft or in future efforts – to strengthen HIPAA enforcement.

- There is an appropriate role for consumer consent in e-health systems, and those systems should be required to honor those consents when they are sought (either to comply with law or voluntarily). But requiring authorization for all data uses provides weak protection for consumers. The approach in the discussion draft moves us further toward securing comprehensive, workable privacy and security protections for electronic health information systems.

Comprehensive Privacy and Security: Critical for Health Information Technology

Version 1.0 – May 2008

In this paper, CDT calls for the adoption of a comprehensive privacy and security framework for protection of health data as information technology is increasingly used to support exchange of medical records and other health information. CDT believes that privacy and security protections will build public trust, which is crucial if the benefits of health IT are to be realized. In CDT's view, implementation of a comprehensive privacy and security framework will require a mix of legislative action, regulation and industry commitment and must take into account the complexity of the evolving health exchange environment.

Privacy and Security Protections are Critical to Health IT

Health information technology (health IT) and health information exchange can help improve health care quality and efficiency, while also empowering consumers to play a greater role in their own care. At the federal and state levels, policymakers are pushing initiatives to move the health care system more rapidly into the digital age.

However, health IT initiatives pose heightened risks to privacy. Recent breaches of health information underscore that the risks are real. At the same time, there is widespread confusion and misinterpretation about the scope of current health privacy laws. Some are pushing for quick "fixes" to try to address the public's privacy concerns, but fully resolving these issues requires a comprehensive, thoughtful and flexible approach.

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.

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 – because they believe such access is likely to increase their quality of care. At the same time, people have significant concerns about the privacy of their medical records. In a national survey conducted in 2005, 67% of respondents were "somewhat" or "very concerned" about the privacy of their personal medical records.[19] 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;

[19] National Consumer Health Privacy Survey 2005, California HealthCare Foundation (November 2005) (2005 National Consumer Survey).

- 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
- 53% were concerned about insurers gaining access to this information.[20]

Appropriate privacy protections must be incorporated from the outset in the design of new health IT systems and policies. 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 than building it at the start. Now—in the early stages of health IT adoption—is the critical window for addressing privacy. As an Internet policy organization and privacy advocate, CDT brings a unique perspective to these issues, based on our experience in shaping workable privacy solutions for a networked environment. In this paper, we describe why it is necessary that all parties—from traditional health care entities and new developers of personal health records, to legislators and regulators—address privacy and security in health IT systems. We emphasize that all stakeholders need to begin immediately to implement and enforce a comprehensive privacy and security framework in all of the various tools and processes of health IT.

The Consequences of Failing to Act

Protecting privacy is important not just to avoid harm, but because good health care depends on accurate and reliable information.[21] 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.[22] 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 disclosed.[23] 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.[24]

---

[20] Study by Lake Research Partners and American Viewpoint, conducted by the Markle Foundation (November 2006) (2006 Markle Foundation Survey).

[21] 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).

[22] Protecting Privacy; Promoting Health/Protecting Privacy; 2005 National Consumer Survey.

[23] Harris Interactive Poll #27, March 2007.

[24] 2005 National Consumer Survey.

People who engage in privacy-protective behaviors to shield themselves from stigma or discrimination often pay out-of-pocket for their care; ask doctors to fudge a diagnosis; switch doctors frequently to avoid having all of their records in one location; lie; or even avoid seeking care altogether.[25] The consequences are significant – for the individual, for the medical community, and for public health:

- The quality of care these patients receive may suffer;
- Their health care providers' ability to diagnose and treat them accurately may be impaired;
- The cost of care escalates as conditions are treated at a more advanced stage and in some cases may spread to others; and
- Research, public health, and quality initiatives may be undermined, as the data in patient medical records is incomplete or inaccurate.[26]

Health IT Can Protect Privacy – But Magnifies Risks

Health IT has a greater capacity to protect sensitive personal health information than is the case now with paper records. For example, it is often impossible to tell whether someone has inappropriately accessed a paper record. By contrast, 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 for appropriate purposes without needing to create large, centralized databases of sensitive information that can be vulnerable to security breaches. Encryption can help ensure that sensitive data is not accessed when a system has been 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.[27]

At the same time, the computerization of personal health information—in the absence of strong privacy and security safeguards—magnifies the risk to privacy. As the recent spate of large-scale privacy and security breaches demonstrates, serious vulnerabilities exist now. Tens of thousands of health records can be accessed or disclosed through a single breach. Recent headlines about the theft of an NIH laptop loaded with identifiable information about clinical research subjects, and the accidental posting of identifiable health information on the Internet by a health plan, underscore these concerns, and are just two of numerous examples. The cumulative effect of these reports of data breaches

[25] Protecting Privacy; 2005 National Consumer Survey; Promoting Health/Protecting Privacy.

[26] Id.

[27] See For The Record: Protecting Electronic Health Information, Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure, Computer Science and Telecommunications Board, National Research Council (National Academy Press, Washington, DC 1997) for a discussion of the inability of systems to be 100% tamperproof.

and inappropriate access to medical records, coupled with the 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.[28]

Elements of a Comprehensive Privacy and Security Framework That Will Build Public Trust, Advance Health IT

A comprehensive privacy and security framework must be implemented by all stakeholders engaged in e-health efforts. Such a framework, as outlined by the Markle Foundation's Connecting for Health, would:

- Implement core privacy principles;
- Adopt trusted network design characteristics;
- Establish oversight and accountability mechanisms.

Congress should set the framework for national policy through legislation. 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. The framework should be implemented in part by strengthening the HIPAA Privacy Regulation for records kept by the traditional health system participants, but also needs to address the increased migration of personal health information out of the traditional medical system.

Notwithstanding the urgent need to address privacy, health information policy initiatives - both legislative and administrative – are moving forward without addressing privacy and security at all, or they are taking a piecemeal approach that too narrowly focuses on a single activity, such as e-prescribing, or on just one aspect of fair information practices, such as the appropriate role of patient consent.

In developing a 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, most notably the HIPAA Privacy Regulation, which established the first federal health privacy framework.[29] While there is no single formulation of the "FIPs," the Common Framework developed by the Markle Foundation's Connecting for Health initiative, which includes broad representation from

[28] See http://www.cdt.org/healthprivacy/20080311stories.pdf for stories of health privacy breaches and inappropriate uses of personal health information.

[29] Other potential sources for policy recommendations include the GAO, the National Center for Vital Health Statistics and the National Governor's Association State Alliance for eHealth.

across the health care industry and patient advocacy organizations, describes the principles as follows:

- 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 change, 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 Connecting for Health Common Framework also sets forth characteristics for network design that can help ensure health information privacy and security.[30] These network design characteristics facilitate health information exchange not through centralization of data but rather through a "network of networks." Such a distributed architecture is more likely to protect information. Other key elements of such a system are interoperability and flexibility, which support innovation and create opportunities for new entrants.

The Role of HIPAA in the New Environment

The federal privacy and security rules that took effect in 2003 under the Health Insurance Portability and Accountability Act (HIPAA) reflect elements of this framework and provide important privacy protections governing access, use and disclosure of personally identifiable health information by some entities in the health care system. 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:

- State and regional health information organizations or health information exchanges (also known as RHIOs or HIEs), which may aggregate and facilitate exchange of personal health information, are often not covered by HIPAA's Privacy Rule.

- Personal health records and other consumer access services now being created by third parties, including companies such as Google and Microsoft, as well as by employers usually fall outside of the HIPAA rules.

- 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, 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.

- While the Privacy Rule includes criteria for de-identifying data, new technologies are making it much easier to re-identify once de-identified health information and to combine it with personal information in other databases, making it more likely that sensitive health information will be available to unauthorized recipients for uses that have nothing to do with treatment or payment.

---

[30] See www.connectingforhealth.org for more details on the Common Framework.

In addition, the HIPAA rules have never been adequately enforced. The HHS Office for Civil Rights (OCR), charged with enforcing HIPAA, has not levied a single penalty against a HIPAA-covered entity in the nearly five years since the rules were implemented, even though that office has found numerous violations of the rules.[31] Historically, states have filled the gaps in federal health privacy laws by enacting legislation that provides stronger privacy and security protections for sensitive data, such as mental health and genetic information. The states continue to have an important role to play, but relying on the states to fill deficiencies in HIPAA's Privacy Rule – or to regulate entities outside of the traditional healthcare sphere – does not provide a comprehensive, baseline solution that gives all Americans adequate privacy and security protections, and does not offer all the entities in the e-health space a predictable and consistent policy environment.

National Conversations about Privacy and Security Have Been Too Focused on the Issue of Individual Consent

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.[32] However, consent is not a panacea. 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.

Among other reasons, a consent-based system places most of the burden of privacy protection on patients at a time where they may be least able to make complicated decisions about use of their health data. Most don't read the details of a consent form and those that do often do not understand the terms. Many wrongly assume that the existence of a "privacy policy" means that their personal information will not be shared, even when the policy and the accompanying consent form say just the opposite.[33] If mere patient authorization is all that is needed to share data with third parties, highly sensitive patient information will be disclosed to entities that are completely outside the scope of the

[31] "Effectiveness of medical privacy law is questioned," Richard Alonso-Zaldivar, Los Angeles Times (April 9, 2008) http://www.latimes.com/business/la-na-privacy9apr09,0,5722394.story.

[32] 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.

[33] See "Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware" (with Nathan Good, Rachna Dhamija, Jens Grossklags, Steven Aronovitz, David Thaw and Joseph Konstan), presented at the 2005 Symposium on Usable Privacy and Security (SOUPS), also in ACM INTERNATIONAL CONFERENCE PROCEEDING SERIES; VOL. 93, PROCEEDINGS OF THE 2005 SYMPOSIUM ON USABLE PRIVACY AND SECURITY, Pittsburgh, Pennsylvania (2005); 2005 National Consumer Survey; " Research report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace," Joseph Turow. Deidre K. Mulligan & Chris Jay Hoofnagle, Survey conducted by University of Pennsylvania Annenberg School for Communications and UC-Berkeley Law School's Samuleson Law, Technology and Public Policy Clinic 2007.

HIPAA privacy regulation. If consent becomes the focus of privacy protection, it is clear that patients will be exposed to unregulated and potentially uncontemplated uses—and misuses—of their data. Further, if reliance on consent by an individual for any particular use of his or her information is treated by policymakers as the key to privacy protection, the healthcare industry will have fewer incentives to design systems with stronger privacy and security protections.[34]

All Entities Should Adopt and Implement a Comprehensive Privacy and Security Framework

Regardless of whether or not Congress takes action to address these issues, states and entities developing health information exchanges and other health IT initiatives should commit to adoption of the comprehensive privacy framework outlined here. Guidance for policy development for health information exchanges can be found, for example, in the Common Framework developed by the Markle Foundation's Connecting for Health Project. Consumer access services such as PHRs must also implement the comprehensive framework through rigorous privacy and security protections.[35] Such entities should make their privacy commitment explicit in a published privacy notice. Consumers should look for these promises and should measure them against the framework. Once companies make a privacy promise, they will be bound to it under the Federal Trade Commission Act. In addition, consumer rating services can compare and assess privacy practices, measuring them against the principles outlined here.

Congress Should Establish a Comprehensive Health Privacy and Security Approach

Although states and the private sector should not wait for action by Congress to protect privacy, CDT believes that Congress should establish national policy to ensure that health information technology and electronic health information exchange is facilitated by strong and enforceable privacy and security protections.
According to recent surveys:

- 75% believe the government has a role in establishing rules to protect the privacy and confidentiality of online health information;

---

[34] By contrast, a comprehensive approach puts the principal burden on the entities holding personal health information to protect privacy by placing clear enforceable limits on the collection and use of personal health information and backs it up with strong enforcement. See Beyond Consumer Consent: Why we need a Comprehensive Approach to Privacy in a Networked World, http://www.cdt.org/healthprivacy/20080221consentbrief.pdf.

[35] See, e.g. the Best Practices for Employers offering PHRs http://cdt.org/healthprivacy/20071218Best_Practices.pdf.

- 66% say the government has a role in establishing the rules by which businesses and other third parties can have access to personal health information; and
- 69% say the government has a role in encouraging doctors and hospitals to make their personal health information available over the Internet in a secure way.[36]

One of the major challenges in developing a comprehensive privacy and security framework is to integrate any new rules with the HIPAA privacy and security rules. Congress should consider both strengthening HIPAA where appropriate and establishing additional legal protections to reach new actors in the e-health environment. Congress should set the general rules – the attributes that a trusted health information system must have – based on the Fair Information Practices discussed earlier. Further, Congress should hold a series of hearings on some of the more difficult issues to resolve and develop a full record that will serve as the basis for more specific legislative action. In particular, Congress should consider:

- The appropriate role for patient consent for different e-health activities;
- The ability of consumers to have understandable information about where and how their Personal Health Information (PHI) is accessed, used, disclosed and stored;
- The right of individuals to view all PHI that is collected about them and be able to correct or remove data that is not timely, accurate, relevant, or complete;
- Limits on the collection, use, disclosure and retention of PHI;
- Requirements with respect to data quality;
- Reasonable security safeguards given advances in affordable security technology;
- Use of PHI for marketing;
- Other secondary uses (or "reuses") of health information;
- Responsibilities of "downstream" users of PHI;
- Accountability for complying with rules and policies governing access, use, and disclosure, enforcement, and remedies for privacy violations or security breaches;[37] and
- Uses and safeguards for de-identified information.

Congress Also Should Enact Legislation to Strengthen HIPAA For Health System Entities

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

[36] 2006 Markle Foundation Survey.

[37] See the Common Framework, www.connectingforhealth.org.

could take to fill some of the gaps in HIPAA. For example, Congress can take a number of actions to secure more meaningful enforcement of the HIPAA rules, including:

- Strengthening Office for Civil Right's (OCR's) role by requiring it to conduct periodic audits of covered entities and their business associates to ensure compliance with the rules;
- Increasing the penalties associated with failure to comply with key provisions of the HIPAA rules;
- Increasing resources dedicated to HIPAA enforcement;
- Requiring OCR to report to Congress on a regular basis on enforcement of the rules; and
- Amending HIPAA to allow for enforcement of the rule by state authorities (such as attorneys general).

Congress should also consider enacting legislative provisions to:

- Establish notification requirements and penalties for data breaches;
- Strengthen the existing HIPAA rules requiring express authorization for use of patient identifiable data for marketing; and
- Require electronic health systems to provide consumers with access to their health information in an electronic format.

Although it is desirable for Congress to enact legislation that fills some of the gaps in HIPAA and to enact a general privacy and security framework to govern health IT, it will be impossible for Congress to legislatively adopt comprehensive rules that fit all of the various actors and business models in the rapidly expanding and evolving e-health environment. Therefore, a second major challenge for Congress is to decide what can be legislated and what must be delegated to agency rulemaking – and what areas are best left to be developed and enforced through industry best practices.

Strengthening Privacy and Security Will Also Require a More Tailored Regulatory Approach

While Congress should establish a strong framework for health privacy and security, it must avoid a "one size fits all " approach that treats all actors that hold personal health information the same. The complexity and diversity of entities connected through health information exchange, and their very different roles and different relationships to consumers, require precisely tailored policy solutions that are context and role-based and flexible enough to both encourage and respond to innovation. For example, it makes little sense to have the same set of rules for "personal health records," which are often created by and controlled by patients and held by third party data stewards outside the healthcare system, and for "electronic health records," which are created and controlled by health care providers for purposes of treatment and care management. To take another example, rules for use of personal health information for treatment need to be quite different than rules for marketing or other secondary uses. Rules regarding use of health information for research need to be separately considered as well.

Congress should not attempt to develop all of the details in legislation. Rather, Congress should enact legislation specifically recognizing the importance of the privacy rights in health information across technology platforms and business models, setting out principles and attributes to guide one or more regulatory agencies in developing detailed, context-specific rules for the range of entities that collect, use and distribute personal health information in the new interconnected healthcare system. One approach would be to direct the Department of Health and Human Services to strengthen the HIPAA regulations that apply to traditional players in the health system, while also directing HHS or possibly the Federal Trade Commission to issue regulations to govern the handling of personal health information by new players who are part of the broader Internet marketplace and not part of the healthcare system. If more than one agency is to be involved, Congress could require them to work together to avoid issuing conflicting rules (as the financial services regulatory agencies did in developing security rules for financial information).

Tasking HHS and/or the FTC with the responsibility for developing detailed regulations allows for:

- A more tailored, flexible approach that will ensure comprehensive privacy and security protections in a myriad of different e-health environments, and
- More regular, active monitoring of developments in the marketplace and a more rapid response to newly emerging privacy and security issues.

Congress should maintain strong oversight over the regulatory process by:

- Requiring regulations to be developed within a particular timeframe;
- Requiring satisfactory completion of the rulemaking before federal HIT grants can be made;
- Mandating reporting by the agencies on implementation and enforcement; and
- Vigorous oversight and reporting on implementation and enforcement.

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. Congress should set the framework for privacy and security by strengthening enforcement of existing law and ensuring that all holders of personal health information are subject to a comprehensive privacy framework. Congress can also take immediate steps to strengthen existing privacy rules, for example, empowering consumers to play a greater role in their healthcare by mandating electronic access to their health records. Given the broad array of entities in the e-health arena, the technological changes in the marketplace today, and the prospects for rapid innovation, much of the details of that framework should be worked out through the regulatory process. The challenge for policymakers is to find the right mix of statutory direction, regulatory implementation, and industry best practices to build trust in e-health systems

and enable the widespread adoption of health IT.

CENTER FOR DEMOCRACY & TECHNOLOGY

FOR MORE INFORMATION

Please contact:
Deven McGraw
Director, CDT's Health Privacy Project
202-637-9800
http://www.cdt.org

Mr. PALLONE. I thank all of you for your opening statements. We will now turn to questions, and I will start with myself for 5 minutes.

The Department of Health and Human Services seeks to fully privatize the American health information community, which currently exists as a Federal advisory committee to define and make recommendations on the future direction and national strategy for health information technology. The administration seeks to make that entity into a private, independent entity referred to as AHIC 2.0; and the private entity is required to be self-sustaining financially, so it could be based, I fear, on a pay-to-play model.

The discussion draft provides for a stronger Federal role in the development of policies and standards, including Federal oversight over timeliness of the process. My concern is that privatizing this entity would be a step backwards from building meaningful consensus and adopting uniform standards for HIT. My concern basically is that privatization of AHIC could undermine a consumer voice.

So I want to start with Dr. Thames. Can you talk about the dangers of fully privatizing a body that will make policy and technical standards recommendations and how that could affect the consumer voice?

And then I was going to ask Ms. Dare to comment on it—to respond to that as well.

Dr. THAMES. Mr. Chairman, I think we would agree with your concerns about a fully privatized service that doesn't have standards that have been set, like we are talking about being set in this draft being provided, and government oversight for that kind of information.

The bill, the draft that we are looking at which requires that these standards' strategic plans be drawn up and that we go ahead with being able to schedule the privacy requirements that we need, we think that is a government-developed—be better government-developed standards with input from people like you have on this panel today.

Mr. PALLONE. Thank you.

Ms. Dare, did you want to respond too?

Ms. DARE. Thank you. We would suggest and observe that all of the evidence today says the best results have come with public-private partnerships. And we can see that with the current work with AHIC, with CCHIT, even the NHIN pilot where the government has played a role in the private sector; so we would want to see a continued role for government in the standards development process.

We would also like to see very much the continued involvement of Congress in knowing the standards development progress and annual reports from whatever entity becomes AHIC 2.0.

So we think the bill speaks very well to broad stakeholder representation. The bill defines the variety of people to be involved in both the policy and Standards Committee. We think that it is vitally important and should include consumers. And I think the bill speaks well to a structure that is both public and private in its approach.

Mr. PALLONE. All right. Thanks.

My second question: you know, I hear a lot from doctors or providers in general about the cost of HIT; even though they support it, where are they going to get the money up front?

According to Health Affairs, the purchase of an electronic medical records system for a solo or small group practice averages $43,000, and the range is between $14,000 and $63,000 in 2005. The costs obviously could be a burden on solo or small group practices, and I was going to start with Dr. Stack and ask you to discuss whether the AMA supports the grants and loans that are in the discussion draft and what you think the impact would be on the smaller solo, rural, or urban practice? What kind of benefits can a doctor expect to see in costs or quality of care and in efficiencies for the investment in electronic medical records they make?

So are these costs legitimate? Do you think in the bill we are addressing them properly and will their benefits accrue so it makes sense for these types of practitioners?

Dr. STACK. The dollar figures that you reference are ones we agree with entirely. There are ongoing costs, of course, for maintenance and service which, rounding numbers, could be in the ballpark of $9,000 per physician a year or some other figures we have seen. These are direct financial acquisition costs and maintenance costs.

The other costs that are more complex to discuss are those that require staff training, process change, change management which involves often a pronounced diminishment of efficiency for some periods of weeks or months during the incorporation of a whole new system and process. It is one of the reasons you emphasize that the standards are so important, because when physician practices make this transition, it is absolutely imperative that that transition has a reasonable likelihood of sticking and serving them well for some period of years. They just simply can't go through that kind of change repetitively. So those financial costs, both direct and indirect, are very real.

In an organization as big as, say, Kaiser where Mr. Ferguson works they can have in-house HIT specialists to help them to direct and purchase and make decisions and then troubleshoot during the implementation phase. In a small physician practice, often the director of human resources, the purchasing director, the coding and billing supervisor, the technology expert, all of those people reside in one person in the form of a physician who really, quite frankly, is far better trained to take care of your health needs than they are all those other functions.

If they are really lucky, they may have one manager for that office to help with all those same tasks. So those costs are essential in the grant programs, and the assistance you have outlined in this discussion legislation are most appreciated, and I think will be absolutely imperative if we are to see success in this.

Mr. PALLONE. Thank you, Doctor.

Mr. Barton.

Mr. BARTON. Thank you, Mr. Chairman. I am in an unusual position in that I am the cosponsor, along with Chairman Dingell and Mr. Pallone, of this bill. So I should be all for it; I should think it is the greatest thing since sliced bread.

And I do think it is a good work product, but I am very concerned about the issue of privacy. I am the co-chairman, along with Mr. Markey, of the Privacy Caucus, so I really want as strong a privacy provision as we can have in this bill. So I listened very carefully to our last two witnesses, and to Dr. Thames earlier when they talked about privacy.

So I am kind of in an unusual position of defending the product, but yet still wanting to improve it if possible. So my first question would be to you, Dr. Thames. Does AARP object if we were to put a definition of privacy into the base bill? We don't have a definition now. And I think Dr. Peel makes a fairly good argument that we should at least have some definition.

Dr. THAMES. I think we would definitely be in favor of your trying to get a definition. What we would, I think—what we are concerned about with privacy from an AARP standpoint is that we don't want to have to choose between privacy and HIT—we want both—and that we feel that relying solely on consent puts an unfair burden on the consumer and overlooks the importance of having the systems and rules and processes to protect the personal health information. And those are the kinds of things that we note with pleasure are in your draft legislation.

So we would look with favor on getting this, but we know that in addition to what is in there in your draft, we are going to have some regulations to make this work. And we don't want to see the bill held up until Congress can decide together what are the right regulations, because they haven't been able to do it in the last 4 years.

Mr. BARTON. I agree with what you just said, but there is no reason we couldn't do both, is there?

Dr. THAMES. No, sir, not as far as we are concerned. There is no reason why we cannot do both unless we fail to work in a bipartisan manner like this committee has done so well up to now, sir.

Mr. BARTON. OK.

Dr. Peel, some of the opponents of your position on strong individual privacy protection say if we were to go down the trail that you advocate, we set up a scenario where we give at some future time a private right of action to sue. What is your evaluation of that?

Dr. PEEL. As far as I know, we have a private right of action to sue for breaches of privacy in all 50 States right now. We are not so interested in exactly what the penalties are for breach of privacy. We are not interested in arguing about private right of action.

I would just like to point out again that consent is very feasible, because we now have technology where you can get consent instantaneously. You can set up broad directives. With technology you could exquisitely decide what gets sent to whom and when, down to the data field. There is smart technology to make consent cheap, easy, and fast and provide audit trails.

So technology—what we are saying is, we want health IT, we want progress with privacy. There is no reason to make a choice. And, frankly, if this draft—if we had this system that is in this draft in effect over the last few decades, two of the most popular presidents in this country, Reagan and Kennedy, their health

records would have been available across the Internet and they never would have been elected if anyone had understood President Reagan's risk of Alzheimer's disease or how sick Jack Kennedy was with Addison's disease.

Mr. BARTON. Dr. McGraw, I read your written testimony when you talked about the need for institutional safeguards. Do you agree or disagree that we could do the institutional part of it and have some sort of an individual consent requirement?

Ms. MCGRAW. We need to do the institutional part of it, and we do think there is an appropriate role for patient consent. It is actually part of fair information practices, and the notion of individual control.

What we disagree with is pinning the privacy and security of the system on patient consent because, in fact, we think that patient consent actually provides weak privacy protections. And I can go into more detail about why I think that.

But at any rate, if you have—the thing with individual consent, if you are combining it with the institutional protections and you are asking folks for their information—I haven't seen a proposal on the table that looks like that, but my sense is that we would focus on whether those institutional protections are there because in our opinion that is what protects privacy and security.

Mr. BARTON. My time has expired, Mr. Chairman. This is something I want to pursue with the stakeholders and also with the members before we go to markup.

Thank you for your courtesy.

Mr. PALLONE. Thank you.

Let me ask unanimous consent to enter into the record a series of statements that have been looked at by both the minority and the majority including the statements from the Divided We Fail Coalition, the Business Roundtable, eHealth Initiative, Consumer Partnership for e-Health, Health Care Leadership Council, the Oregon Institute of Technology, and the Federal Trade Commission.

Without objection, so ordered.

[The information appears at the conclusion of the hearing.]

Mr. PALLONE. And next for questioning is the gentlewoman from California, Ms. Eshoo.

Ms. ESHOO. In the draft discussion, in subtitle (a) in the security provisions, there is a notification in the case of breach. And it goes through to identify that if a breach—if there is a breach of the unauthorized use of information, it could reasonably result in substantial harm, embarrassment, inconvenience, or unfairness to the individual.

Any of the panelists, in taking a look at that language, it strikes me as being a low threshold for notification. This is notification if there is a breach of security.

Does anyone want to weigh in on that? Again, it strikes me as being a low threshold; and I don't know if this were ever challenged in a court—"embarrassment, inconvenience, or unfairness," that is an unusual standard.

Dr. PEEL. I may be wrong, but I think that might come from California's breach notice.

Ms. ESHOO. I don't think so, no.

Ms. DARE. If I might, Congresswoman, we echo your concern that the language is at least unclear and the standard unclear. We think information that speaks more to significant harm, risk of medical fraud, identity theft, unlawful conduct, gives everybody a more succinct and consistently applied standard.

Ms. ESHOO. Mr. Ferguson had his hand up.

Mr. FERGUSON. I would like to add and agree that we think the California law is a lot clearer as to when you have to notify . And we follow the California breach notification in all of our locations across the country.

We also think, though, that the breach notification provisions should be the same for all personal health databases regardless of whether they are held by PHR vendors or by covered entities.

Dr. PEEL. I just remembered, that language is from OMB. I knew I had seen it somewhere.

Ms. ESHOO. I didn't think it was California. That is helpful, what each one has said, and I think the committee staff is going to have to take note of that in the draft discussion.

On the issue of safe harbor that was mentioned by Ms. McGraw, I think the committee bill should allow safe harbor to apply to both PHRs and covered entities, and I wondered if you might add on that.

Ms. MCGRAW. Sure. We agree with you.

There are two slightly different standards with respect to a breach that occurs with a PHR versus in the traditional health care context. You know, the California data breach law that was mentioned, essentially the trigger for notification is whether or not the information was encrypted or not. So without having to go through—will this person be embarrassed by this information, because I do think you need to actually have a different threshold than you do for financial data. The amount of money in your bank account is a completely different piece of information about you than the fact that you last week had to take an STD test. So it has to be a different trigger, and it is hard to get to that trigger.

So you mentioned a low-threshold issue, but the encryption, if for no other reason than it actually provides an incentive for organizations that hold data to encrypt it—and Ms. Dare mentioned not encryption, but something else—I think be willing to think about whether we want to lock ourselves into a particular form of technology. But I still think it is a good idea to build those incentives in by creating a safe harbor or rebuttable presumption.

Ms. ESHOO. Thank you. I appreciate that.

In the discussion draft it requires notification of individuals whose health information has been breached or wrongfully disclosed, but the draft specifies that the notice be provided in writing by First-Class Mail; and I think that this is a real irony because we are talking about HIT, because it seems to me that the central purpose of health information technology legislation is to move away from what that says.

Everybody is smiling. We all get it.

Does anyone think that snail mail should be the default method of communication in cases of a data breach?

Dr. STACK. It may be sufficient to say, I think there would be consensus that it is a little archaic.

Ms. ESHOO. I will take that. I think those are my questions for now, Mr. Chairman. And did you already stipulate that we can submit questions?

Mr. PALLONE. If you want to ask questions, absolutely any member who would like to submit questions for the record.

Ms. ESHOO. Thank you very much everyone. I think this has been enlightening; and I think that there are obviously some areas where we are going to be changing the draft based on some of the things that have been brought up today, which is what this hearing is terrific for. So thank you.

Mr. PALLONE. Thank you.

Next is the gentleman from Texas, Dr. Burgess, for questions.

Mr. BURGESS. Thank you very much, Mr. Chairman. Thank you.

Ms. Dare, let me welcome you from Richardson, Texas. It is always good to have a Texan on the panel; that way I know it is going to be fair.

Let me just ask you if this bill were to suddenly be on the President's desk and signed, how would your life change at Cisco Systems? What would be different? What are the things that are embodied in this legislation that would make things better for you and what are the things that would make things worse?

Ms. DARE. Thank you for that question. It is a very broad one, and I always start to consider both Cisco as an employer and the employees for whom we care passionately about health care, as well as our technology perspective.

I would say from the technology perspective, most initially, we would hope the bill would accelerate the development of the regional health information exchange networks and that we would see much better connectivity and collaboration across the continuum of care, whatever the organizational body might be.

Mr. BURGESS. Can I ask you a question on that? Under development right now, even without any Federal legislation, are there not companies out there who are working on those issues of interoperability, how to get one system to talk to another? Is that work not ongoing at the present time?

Ms. DARE. It is, and I would add, as well, the most meaningful piece of that work really comes together in the four pilot projects that the Federal Government has helped sponsor and fund where you really bring together—and they are each different and use different technology approaches—but where they are, in fact, proving today that across different communities, using different technology approaches, you can share health information technology effectively and securely.

It is a huge undertaking. The longest standing, successful project of that type is in Indianapolis, and they have been doing it a long time and have been successful for some unique circumstances. But if we want to see that movement take momentum across the country, we think you do need legislation like this and you need the sponsorship, the convening role of the government, to help bring some of these bodies together.

We have seen in the last 4 years the work around these sort of regional collaboratives accelerate significantly versus the 8 or so years before that when the work in Indianapolis began. In fact, there were significant undertakings in communities like Santa Bar-

bara which attempted to do very good work and, in fact, struggled and have now disbanded.

It is an evolving territory, but one we think this bill can make a big difference for.

Mr. BURGESS. Like so many other areas, there is a need, there is a market for that technology. Technology has already been referenced at several points and I suspect a company like yours would be anxious to fill that niche and claim that market share.

We talked a little bit about the irony of having the notification come through snail mail. Part of the irony of having the Federal Government in charge of this type of capacity, this type of capability, is we have the system today where the VA, under the VistA System, can't communicate with the Department of Defense. So the bad stories that came out of Walter Reed Hospital 18 months ago largely were generated by the fact that, well, guys were on medical hold, their records that they were preparing for the VA would get lost and they had to rely on paper records because their DoD records could not electronically transfer.

So I am a little suspect of our ability at the Federal level to create a system that actually works because I have been in communication with the folks in the Department of Defense and this has been an ongoing problem for 18 months and I don't see us quite there yet. Yet I see efforts in the private sector where they recognize the need for this. In our neck of the woods, Presbyterian Hospital and Baylor Hospital looked at a merger 10 or 15 years ago and couldn't do it because they didn't have the interoperability to their computer systems.

So clearly the market exists for that type of capacity. I just wonder if we are making a mistake by putting ourselves in between what should be a private sector niche to fill and saying don't worry about that because we are going to take care of it at the Federal level. I have heard that for 5 years since I have been here and I don't see us any closer today than we were 5 years ago. But maybe I am just being too critical.

Dr. Stack, I didn't want the time to expire without asking you—I think we heard reference to the RAND Corporation study about health information technology, the $77 billion we are going to save in the year 2015. Of course that study always ignores the investment that is made by what you so eloquently put in your testimony, the small medical practitioners, the small businesses that are out there, and then of course you provide some data, the cost for that.

In the RAND study, if I am correct, they did talk about incentives for the health care provider community doctors, that those incentives would have to be early, they would have to be limited. You didn't want to reward late responders by continuing to offer that help well down the road. But the most critical thing that is often overlooked is those incentives have to be substantial. They have to be substantial for all of the reasons that you outlined in your response to Mr. Pallone's question, the fact that there is a significant outlay of capital in what is generally a fairly capital intense activity anyway, which is a running of a small practice. And there is the training, there is the ongoing maintenance and then the fact that some of us are slow. And it adds minutes to each patient en-

counter. And if you add a few minutes to each patient encounter when you have to see 30 to 45 patients a day to make the cashflow work, you are suddenly talking about a couple of hours added onto the day which are not available for patient care, revenue generation, or time with family.

The other issue on the telephonic aspect of this——

Mr. PALLONE. Mr. Burgess, are you going to ask him a question? Because you are a minute over.

Mr. BURGESS. I actually just wanted to thank you for bringing that up. And on the RAND Corporation issue about that substantial incentive, I hope that you and your friends at the AMA will continue to look at that and provide us with real data as to just how substantial those incentives must be.

Mr. PALLONE. Do you want to respond?

Dr. STACK. In the absence of a question, thank you for the opportunity to comment additionally. I would like to note that I was intentionally silent on the potential and prospective cost savings because depending upon what lens you frame that, you can find fantastic savings or minimal savings. I think what the true value here is—and Secretary Leavitt has commented on this—is transparency in the health system. And all these issues intertwine in that to a great extent.

The answer to privacy problems is to hold people accountable for proper access and responsible use of information. Addressing privacy as the cause when the issue is really that health plans—it is inconvenient to take expensive beneficiaries because they cost money and increase medical loss ratios. Hiding that information, which is necessary to care for people, is not the way to address it. The way to address it is to find the fundamental issue, which is how the information is being used and what is done with it.

In your instance, having to do with the costs of this, having more information in the hands of clinicians and people who help to manage this health sector—and it is questionable if it is a system at this point and people have made that comment already about a health sector. I don't think we know the true power that we could have potentially to find opportunities for cost savings, quality improvement, safety improvement. That is the fantastic promise of health information technology and why it is so important to help the Federal Government at a high level, broad level, align incentives for the private participants in this system but try not to delve too low down so that the private sector is stifled in its ability to innovate and deliver a better result.

Mr. PALLONE. Thank you.

Mr. Waxman.

Mr. WAXMAN. Thank you very much, Mr. Chairman. Although our current Federal health policies provides for criminal and civil penalties against those who violate the privacy provisions and under the rule the Secretary of Health and Human Services can impose civil penalties and he can refer cases to the Justice Department to pursue criminal prosecution, the privacy rule has now been in effect for half a decade and there have been 30,000 or so complaints alleging violations reportedly filed with HHS, yet I understand there has not been one instance in which HHS has imposed a civil penalty for a violation of the rule and the Department of

Justice has prosecuted only a handful of criminal cases regarding the rule.

This history underscores, it seems to me, the need for creating additional enforcement mechanisms to ensure an effective Federal and health privacy protection scheme. Toward that end, I am interested in exploring the role State attorneys general might play in enforcing medical privacy protections. It is my understanding that under current law some State AGs may have authority to pursue criminal penalties for HIPAA violations, depending on the State statute governing the AG's authority. But it is less clear that State AGs have authority to pursue civil penalties for HIPAA violations.

Ms. McGraw, is that understanding correct? And what do you think we ought to be doing about it.

Ms. MCGRAW. Yes, it is my understanding. If you read the penalty provisions of HIPAA, they are actually not in the regs. They are actually in the statute, and the authority to impose the civil monetary penalties is vested in the Secretary through the Office of Civil Rights. So arguably one could argue that that statutory construct creates exclusive authority to civilly enforce the law with the Secretary versus on the criminal side it doesn't vest the authority with any particular body and it doesn't expressly give the State AGs the right to act, but in some States they have with respect to their authorization of what their State AGs can do, they could enforce the criminal provisions because that piece of the statute is just written differently.

Mr. WAXMAN. Well, do you think there would be an advantage in ensuring clear authority for State attorneys general to enforce violations of HIPAA?

Ms. MCGRAW. We would endorse that, but we would also counsel the Committee to actually look at those statutory provisions again. Not so much the criminal authority, because I think that that is fairly clear. But when you get to the civil penalty piece, we have been disappointed in OCR's lack of putting a penalty on anyone to date, even though they have found violations of the rule. But the statutory provisions themselves are not written in a way that gives them a tremendous amount of freedom to actually impose those penalties.

And so I would ask the Committee to take a look at that if you are interested in pursuing the enforcement piece, which I think you should because you can create all of the right set of protections in the world but you don't have a right without a remedy. And the remedies are tied to enforcement of the statute by our——

Mr. WAXMAN. You are raising concerns about the existing law and the enforcement by the Secretary under that existing law. I was also posing the idea of letting the State agencies enforce the law. You think both need to be looked at?

Ms. MCGRAW. Yes, I would look at it. Because arguably if you give the State AGs the authority, they have to abide by the statutory provisions that the OCR has to follow.

Mr. WAXMAN. OK. Does anybody else—Dr. Peel, I see you are raising your hand.

Dr. PEEL. Yes, I have a couple of comments. I think the scheme that you are proposing, where the State attorneys general take action, is actually in the Trust Act. But I think there is something

key missing at the table that we have got to talk about, which is that the vast majority of breaches of information today are legal under HIPAA. So most of the complaints turn out to be uses that are allowed under the privacy rule that no one would ever agree with. And because we don't have audit trails, people aren't noticed how far their information goes, it is difficult to even know who has seen your records or for what use because HIPAA allows broad use of information if it falls under treatment, payment or health care operations.

So we have no control over our information according to HIPAA, And so many of the violations turn out to be not real violations under the privacy rule.

Mr. WAXMAN. So even though there were 30,000 complaints, not all of them would be violations? Even though they are enough of a problem that people are complaining about their privacy——

Dr. PEEL. Yes. Yes. Yes. People are concerned about privacy violations and they want help.

Mr. WAXMAN. I would be interested in getting your input and suggestions on how we ought to change that law to make sure that we make clear that some invasions of privacy that concern people should be in violation.

Dr. PEEL. That is why we want you to define privacy and reestablish our rights to control where the information goes.

Mr. WAXMAN. Thank you. Thank you, Mr. Chairman.

Mr. PALLONE. Thank you, Mr. Waxman.

Mr. Deal.

Mr. DEAL. Thank you, Mr. Chairman. I apologize to the panel for my absence in and out today, but I was handling the Community Health Center Reauthorization Act on the floor, and I think all of us understand the importance of that piece of legislation, which we did pass by voice vote. Unfortunately, somebody asked for a recorded vote. So we have to deal with it later in the day. But that was the reason I was gone.

I have listened to my constituents, some of whom have expressed some of the same concerns that many of you have expressed. But from the provider, the health care providers, the doctors' offices, and even some of the companies that have tried to put systems in place, there seem to be some concerns there and I would like to try to focus in on it and, Ms. Dare, I think you may be the one I need to address this to since you deal with the equipment and the hardware kind of side of it.

One of the concerns that many people have expressed is as we craft something here, how do we deal with those maybe individual physician offices or practices that have already put their own systems in place, they already have an electronic medical record in place within their practices? When we talk about grant money and all of that, many of them get concerned about, well, we took the lead, and I have got one firm in my hometown invested a million dollars to put theirs in place. You know, they are concerned, well, we get left out of this process. How do we address making sure that those existing systems become interoperable in the exchange of information from them and should they be considered eligible for funding to make sure that that happens?

Ms. DARE. Thank you for that very important question. I will answer the second part of it first if I might. My immediate thought is to say, yes, for some of the Committee to taking a system that isn't able to exchange information and convert it into one that is. That would seem a perfectly viable and appropriate use of the dollars available for investment in IT systems. I don't think we want to punish the first movers unduly and some of those systems were put in place before interoperability and exchange of information was readily available.

The second part of your question, that front one hinges to a great extent on what kind of systems they have. So those electronic medical records—I use that term deliberately—have been around in health care for 20, 30 years, not widely used obviously. Those older systems predate the Internet or webcon activity, right? So depending on the date of the system and how it is designed, how you make those Internet-enabled or how you provide the right security technologies for them to share information appropriately isn't a question easily answered and it is almost a case-by-case situation.

Mr. DEAL. The more I have talked to people who are in the system, the more I am made aware that this is indeed a complex issue. It is being dealt with many times in a fragmented fashion, but if we are going to craft legislation, the legislation I think has to be comprehensive. So let me ask you about one of those somewhat fragmented approaches.

We have people in companies who have approached it from the standpoint of the patient, the consumer, and whether it be smart cards or whatever you choose to call it, the idea of portable medical records that they can carry with them to whoever provides their health care. Some concerns that come into mind as I talk with my physician friends is, well, how do we make sure that every health care provider updates that card? That is one question. The other question, how do you deal with people who are not thought of in the mainstream such as an independent lab who is doing a test? Do we not have to make sure that however we craft this, that that inclusiveness brings all of these people under that tent or else we either miss important pieces of medical information or what we have is incomplete for one reason or the other?

Mr. Ferguson, you probably have more experience from trying to deal with those issues than anybody else. Let me ask you if you would respond, and I may not have phrased it properly.

Mr. FERGUSON. Thank you for the question. I think that having the broad scope of different kinds of entities covered in terms of these interoperability specifications clearly is very important, and so we would want to look for some way to do that. Now, I think that in terms of the modern medicine just being so complex that it requires IT, I think really means that this has sort of become the cost of doing business. So we think that the implementation of the systems really is going to be demanded by the marketplace in terms of the higher quality cost and computer efficiencies and convenience that are coming being really the incentives for the slower adopters.

Mr. DEAL. Can I just ask one quick follow-up? As an insurance company, when you get a piece of a medical record, let's say from an independent lab that you are paying for under your policy, who

feeds that information into it? Do you as the insurance company do it? Who puts that in the record?

Mr. FERGUSON. Well, the lab results in that particular case, they are ordered by the physician and they would then go from the electronic medical record system out to the lab and then the results come back to the electronic medical record system in the hospital that is then vetted into the system, if you will, by the physician before it can be released to the patient in that particular example. But this is actually a case where the portable device based—whether it is on a card or a thumb drive, that kind of record system can never be complete and up-to-date. So that is one of the reasons why we so strongly support these interoperability provisions and standards for transporting data as needed to present the complete record for patient care.

Mr. DEAL. Thank you. Thank you, Mr. Chairman.

Mr. PALLONE. Thank you, Mr. Deal.

Next for question, the gentlewoman from Wisconsin, Ms. Baldwin.

Ms. BALDWIN. Thank you, Mr. Chairman. Mr. Ferguson, I understand that Kaiser Permanente has been very involved in promoting health IT interoperability and that you have participated in the Certification Commission for Health Information Technology. What I would like to do is ask a couple of questions about the work of that commission and how it would be influenced by the passage of this legislation and the Standards Committee that is proposed. But before I do, for context, can you give us a brief description of the work that the Certification Commission is currently doing?

Mr. FERGUSON. The Certification Commission for Health IT has developed certification criteria for ambulatory electronic health record systems, for inpatient systems, is currently starting work on personal health record systems and also for health networks or health information exchange organizations. And so in each of these areas, there are provisions under the Executive order that is being followed through HHS for these certified systems to be used in different contexts.

Now, I think that one of the things, as I mentioned in my testimony, we would look for additional transition specifications in the legislation for some of the other entities that are involved in that Federal health IT strategy that HSS is currently pursuing. So that would include HITSP, the standards organization, CCHIT, the certification organization, the National Health Information Network, but also the advisory committee, NCVHS I think. So all of those different kind of entities need some sort of transition into the new structure and not really just the policy committee.

Ms. BALDWIN. So can you comment on how you might envision the Certification Commission interacting with the HIT Standards Committee that is created in the discussion draft before us? And also just comment on whether you think it would be serving a complementary purpose or are there some duplicative purposes? And lastly, to give you a laundry list here, lessons learned from the Commission that might be helpful to us in establishing the HIT Standards Committee that is in the discussion draft.

Mr. FERGUSON. I don't think there needs to be any duplication between the proposed Standards Committee and the Certification

Commission if it were to retain essentially a similar purpose and function to what it does currently because the Certification Commission essentially ends up certifying systems against the standards that would be endorsed by the Standards Committee. So I think it is more of a complementary matter rather than duplicative.

Ms. BALDWIN. Any lessons learned that might guide us in examining——

Mr. FERGUSON. We found certainly a healthy tension between different parts of the electronic health records vendor community in terms of being able to move towards the interoperability standards quickly, where different segments of that vendor community have been able to move toward adoption of the interoperability specifications faster than others. I don't know if there was some codification of the requirements for moving to the interoperability standard, if that would help to sort of unify that movement.

Ms. BALDWIN. Thank you.

Mr. PALLONE. Thank you.

The gentlewoman from North Carolina, Mrs. Myrick.

Mrs. MYRICK. Thank you, Mr. Chairman, and thanks to all of you for being here. It has been very helpful. I saw the concept of the draft in doing IT. I think it is critically important that we do that. They want to establish a permanent government office. That at least concerns me. So my question to any of you who wish to answer is, do you see after—if this gets up and running and is implemented, is there really a need for a permanent office? Once the Federal Government has done its job of getting it started and everything is working, do we still need that office?

Dr. PEEL. The only thing I would add is once the system is up and operating, I think there would still always be challenges to security and privacy. So we would like to see someone really have responsibility for protecting citizens and to make sure that these systems really are safe and do what they are supposed to do.

Mrs. MYRICK. And I was going to ask that question next, relative to what you see the role of preventative breaches. But would that only be with regard to the Federal side of it or with everybody, with individuals?

Dr. PEEL. Well, the breach problem is enormous, as you know, and increasing every year. I think there were 200,000 breaches in Georgia in the last 3 years, 2 million in California. We really have a long way to go to make these systems really, really secure. And so—and even industry testing has proven they are not secure. There was an industry group that studied 850 electronic health record systems over 15 months and they couldn't find one that couldn't be hacked or penetrated. So we have a long way to go for health technology to really be safe from hacking.

So that seems to me it would be critically helped with continued coordination and oversight at the Federal level for security, as well as privacy, and we know that new threats are going to be emerge and it would be good to have some coordination and guidance and leadership to make sure that the threats are dealt with in a reasonable fashion. Government hasn't yet, but that would be a great job for the coordinator.

Mrs. MYRICK. But you still see the role for the States and the State IDs?

Dr. PEEL. Oh, yes, absolutely. And that is in the Trust Act actually, language like that.

Mrs. MYRICK. OK, thank you. Anyone else? Dr. Stack.

Dr. STACK. I guess I would look at my LNC reports to the Secretary of HSS, I believe. Is that not correct? So I look at it in a way that the CEO of the largest purchaser of health care in the United States, kind of how that CEO, the Secretary of Health and Human Services, would want to manage their staff. But I think there is going to be a lot of work for a long time to come on HIT and certainly you would want the Federal Government and its cooperative through Medicaid with the State governments to have a point person who could try to most efficiently and intelligently manage that resource. So it is hard for me to say it should be permanently there forever. But the amount of work to be done is not going to diminish as this goes forward.

Mrs. MYRICK. Thank you.

Yes, Ms. Dare.

Ms. DARE. If I might add briefly as well to build on Dr. Stack's previous comment that we have a health care sector but not a national health care system, I think there is huge value in someone having that national perspective in trying to bring a very fragmented health care sector together under some unifying initiatives and a national vision for what HIT can do, and I think that is added value for the permanency of that office.

Mrs. MYRICK. So that is what should take place in effect? OK. Thank you.

Mr. PALLONE. Thank you.

Mr. Rogers.

Mr. ROGERS. Thank you, Mr. Chairman. To me this is one of the most important issues I think we can get bipartisan support on soon to unleash a lot of intellectual and real capital on a real problem. We have a 2008 delivery system in health care and a 1970s administration of health care. And I think this is the great way to do it. I do think and I get a little concerned—and I want to thank Anna Eshoo, by the way, before we get started. We have worked on the bill for about 3 years. And it is bipartisan, bicameral. I see a lot of it is in this product and I hope that we can work together to work out some of the things that we have encountered in the process of putting that bill together. And both our staffs did a great job.

The notion between security and privacy, they are very different problems, very different problems. And I think if we confuse them, we will do more harm than we will ever do good and we will stop the whole benefit of what health IT can bring to be more efficient and really save lives in health care. We have systems in Michigan that have already reported internally huge amounts of lives saved and money as a result because of medical errors that never happened that had happened before under the old systems.

And so I want to direct this to Dr. Peel, because I love your passion for your issue. But one of the things on your Web site struck me and it said, and I quote, the greatest use of your health care records today is to hurt you, not to help you. Do you believe that?

Dr. PEEL. I do, And I will a tell you why. We don't even understand how far information goes. In fact, I hope this committee and Congress will investigate how far data flows. This is the tip of the iceberg. For example, prescription data mining and sale. You know, I talked about that one company that is on the stock exchange that got $2 billion in 2006. We don't even know how many prescription data mining companies there are. We can't figure it out. And we learn things every day about new places where information is being collected and used that people would never imagine. Transcription businesses, where they will—many of them are offshored. It turns out when they get that data, they turn around because they can under HIPAA and they sell the data. Everyone that touches the data——

Mr. ROGERS. Let me ask you this, then.

Dr. PEEL. Everyone that touches the data potentially sells it and many of the electronic——

Mr. ROGERS. I hear you, Doctor. But don't you think it would be better to fix HIPAA than lay a whole other system of privacy over HIPAA?

Dr. PEEL. It doesn't matter to us where we put the fix. We just need the fix.

Mr. ROGERS. That is progress right there. So to say that you would be willing to do that——

Dr. PEEL. You are better at figuring out where and how this should be fixed than we are.

Mr. ROGERS. I wouldn't say that or we would have an HIT bill already. But I do appreciate that and your willingness to try to work with us because that is a very important point to me. If we lay another privacy layer over HIPAA, you might as well forget any savings, any interoperability. It is just not going to happen. And I think that would be a tragedy, an absolute tragedy if we don't come together soon on putting together some kind of health information technology bill that allows—but privacy—by expanding HIPAA, I am there. Nobody wants their records out there.

Dr. PEEL. OK.

Mr. ROGERS. But when you can make sure that we can save lives through medical errors to the tune of—I think it is 79,000 people a year through medical errors in the United States of America, that is a tragedy. And I don't want to have our arguments and debates about the difference between privacy and security stop the saving of 79,000 people who we know the private sector can help us save. And that is my concern about how much effort we are spending here without the true explanation of how much good a health IT bill can do for thousands and thousands of Americans.

And this consent provision I have to tell you worries me a little bit. And I agree, that is why we put a provision in to extend HIPAA to vendors of plans. And I know you don't like it, but I would argue that you should help us try to fix HIPAA versus try to create some confusion on what is a bill we know will save lives and save money.

Dr. PEEL. I would love to help you fix HIPAA. I agree with you completely. And your point about lives being saved with electronic medical records, I completely agree. But you have also got to understand, as I was talking about, millions of people won't come into

my office, won't cross the threshold and get help unless they believe that their information is really safe and only stays with the people that they want to see it. And so there are lots of lives lost. People with delayed treatment for cancer, particularly in my field, people with mental illness. And I didn't even get to talk about the RAND study that showed 150,000 Iraqi vets with PTSD, post traumatic stress disorder, are afraid to get treatment because of privacy concerns. And soldiers know that their treatment and records are not private. I mean, this is a crime. This is unnecessary that these needy people that have sacrificed for us don't feel safe getting treatment because they don't want their futures jeopardized.

Mr. ROGERS. And I understand. And I understand your passion for it. But we need to make sure that emotion doesn't drive the reality of how we can fix that problem.

Dr. PEEL. It is very fixable with technology.

Mr. ROGERS. I absolutely agree. And I think the pretty strong rhetoric on your Web site—now, you say you believe it. I find that very hard to believe that people believe their medical records are there to hurt them. And the consent provision that you advocate for that worries me most is that we don't want to have to get consent from a doctor walking to a nurse or better yet a doctor picking up the phone and saying, I have this case, doctor friend of mine, that I am not sure I understand, I would like you to walk through it. That is called good medical care, I think.

Dr. PEEL. It is not needed for that. I am a practicing physician——

Mr. PALLONE. The two of you are arguing. Let me just stop a minute.

Mr. ROGERS. This is important, Mr. Chairman.

Mr. PALLONE. I understand.

Mr. ROGERS. I want to finish by saying that it is important and rhetoric is important in this debate. And let us all come together to understand if we can work this out without the harsh rhetoric, we will get a bill that will save lots of lives and engage the private sector.

Mr. PALLONE. I think that is a nice conclusion.

Let me move to the gentleman from Texas, Mr. Gonzalez.

Mr. GONZALEZ. Thank you very much, Mr. Chairman. And thank you very much, and members of the committee and the ranking member, for allowing me to participate since I am not a formal member of the subcommittee. Nevertheless, there are many of us that are interested in this particular subject. Many of us have bills out there already floating around. You heard Mr. Rogers, I've got mine and everybody else has one out there. And I guess the way to describe it is I think we have—everybody is ready to dance but the bandleader hasn't started the music. So I am hoping that Chairman Pallone may be that band leader and this is the particular vehicle to start that music so that we can all get along with the project and with the challenges that face us.

The debate that we are having here—and this is what concerns me. I am going to agree with Mr. Rogers here—is that when we go into HIT let us not open the debate to everything else out there and try to fix any and all problems that we have out there that exist only because the medium may be different, paper records and

so on. I don't think that is going to happen. I think it is an opportunity to address shortcomings and if we can, we will. But this may be the committee to actually understand it better than any other committee. We have jurisdiction over telecommunications, we understand the industry, we understand the technology. We have individuals also, as Mr. Waxman and Mr. Markey, that are very, very dedicated to the proposition of privacy. And, of course, we have Mr. Pallone on the health end of it. So let us not waste this tremendous opportunity.

The other thing is, we are talking about we need consumer confidence before maybe we can get this off the ground. Maybe, maybe not. Because I think—I am going to go on the record in a minute and ask Dr. Peel how she feels about what is going on out there where I think consumers are expressing some confidence by utilizing services that are out there presently that are not being offered by the government or the doctors. But the biggest impediment and my greatest concern is the medical profession—and this is to Dr. Stack. The greatest impediments would be, one, the cost. And we hear all we have are grants. But please understand there are other people that are thinking in terms of the Medicare incentives, that are considering the loans, that are considering the tax incentives. There is a reason they are not in this bill for very, very, very good reasons. But we understand we need to expand that particular universe.

The other thing is this market uncertainty. I think Ms. Dare described it that way. Every doctor I talk to says Charlie, if we are going to invest that kind of money, we don't want this thing to be obsolete next year. We want it to be the total interoperability aspect of it. We have all these challenges. What scares me of course is we do get sidetracked with trying to fix every ailment when it comes to privacy and security and, no doubt, electronic medium does increase the risk. I give you that, Dr. Peel. But we have individuals out there. We have an individual from Verizon here. Their CEO is chair of the Business Roundtable on Health and Retirement that have embraced this concept already. We have got Google out there that is providing—and I do want to get to my question now. But hopefully this will preface where I am coming from. Google now offers personal health records on the Web. It is all totally in control of the individual. And they had this out of the Cleveland clinic, it was oversubscribed in SOAH. The Google record he said allows the user to send personal information at the individual's discretion into the clinic record or to pull information from the clinic records into the Google personal file.

Now, remember, this is all motivated, generated, and controlled by the consumer, which is good, which pretty well tells me that they have some sense of security and confidence in some system that is out there that probably allows less than what we are providing under this particular piece of legislation.

In the Cleveland trial—and I am reading this from the New York Times article—patients apparently did not shun the Google health records because of qualms that their personal health information might not be secure if held by a large technology company. Now, what information is shared with doctors, clinics, or pharmacies is controlled by the individual. We have 15, 1,600 people. We are

going to have a lot more people—you watch what happens with what Google is offering out there.

So, Dr. Peel, I am just curious, why would so many people be willing to subscribe to this service? They see the value of it. The clinics, the practitioners see the value of it. If they had such concerns that they are just letting this information out there into cyberspace, that it may be shared by millions and millions of curious people?

Dr. PEEL. I would love to answer that. First of all, I think part of the reason people are willing to use the Google system is they strongly promise privacy. They strongly promise to control what happens to your records. Now, as you can already tell, we are suspicious. Maybe that is true. Maybe that is true. But I think it is the promise of control that they feel will help to drive acceptance. And let me just point out I know a little bit more about the Microsoft health vault system because Microsoft's business model for the health vault system is to adhere to all of the 11 privacy principles that our bipartisan Coalition for Patient Privacy suggested be put into health IT legislation. Microsoft feels that that is the model that is going to drive adoption of health technology, is really empowering the patient to control where the data goes. And going further than that, Microsoft——

Mr. PALLONE. We are a minute over.

Dr. PEEL. I am sorry.

Mr. GONZALEZ. And I apologize, Mr. Chairman. Ms. Peel, we can follow up this conversation in the future and I would appreciate it. Thank you very much for your indulgence, Mr. Chairman.

Mr. PALLONE. Sure. Mr. Markey.

Mr. MARKEY. Thank you, Mr. Chairman, very much. And congratulations on your work and Mr. Dingell's and Mr. Barton's and Mr. Deal's on this bill. And I also want to thank Mr. Barton for mentioning the fact that he and I founded the bipartisan Privacy Caucus about 10 years ago and we have teamed up on adding privacy provisions to just about every bill that has come through here over that 10-year period and I am looking forward to doing the same thing here because I do think we have a privacy crisis in the country and it would be a tragedy if we didn't build the privacy principles into this bill. I love Google, I love Microsoft, and I love all the high-tech firms in my district. And if any of them want to provide high quality privacy, God bless you. And why would they object then to having a law that said that everyone else had to provide it, too? And I think that is how we have to view it. We will take whatever the standard is to Google users or whoever and we will say, good, we will mandate that, then. Huh? Do you have a problem with that? I don't think they will say they will, to be honest with you. I don't think the problem is with the technology companies. I think the technology companies will do this in a second. I think the problem is the insurance companies, it is these big HMOs. That is where the problem is. OK? It is not a technological issue. This can be done. It can be done quite simply. It can be done for a relatively low cost and all the high tech firms will move in and solve the problem. The problem is that the insurance firms and the other firms want to make money off of our privacy, they want

to make money off of our medical secrets. They want to market our medical secrets to other companies and make dough off of it. OK?

So that is our challenge. It is not a technological challenge at all. It is a challenge of whether or not we are going to say to every family in America when you hand over your medical records, they are protected unless you want to give up the privacy. And if you don't, then forget it. But what the hell, if you have got a broken wrist, what the hell do your psychiatric records have to do with this? Should they gain access to every single medical record you have if you are going in for a broken wrist? I don't think so.

So, I have always said it and I will say it again, I will give my right arm to get privacy into the HIT bill and here is where I am right now. So, Dr. Peel, in your testimony, you have noted that as a practicing psychiatrist some of your patients have suffered significant consequences as a result of privacy breaches. What specific security and privacy protections in health IT systems do you think would make it less likely for such breaches to occur?

Dr. PEEL. Well, we think we need state of the art security. And in terms of privacy, a bipartisan coalition came up with 11 basic privacy principles, which were really frankly in the amendment you proposed to H.R. 4157 in 2006. That basically incorporated all the kinds of protections we wanted. And we thank you very much for the Trust Act, which once again incorporates even more than the basic principles that were in your amendment to H.R. 4157. These we really believe—consumers really believe are what it is going to take for trust in this kind of a system and environment.

Mr. MARKEY. Thank you. And by the way, right now I have already got game one of the Celtics versus the Lakers TiVoed on my TV set. I mean, how complicated this is with modern technology. You can get it all set 3 days in advance. This is a simple thing to say protect this person's privacy. OK? They haven't given us permission to send it to anyone else. It takes 10 seconds to get it done.

Question number two. As you know, in 2005, California State regulators fined a division of Kaiser Permanente for exposing on the Internet the confidential health records of about 150 of its patients for as long as 4 years. At the time, the director of the California State agency that levied the fine, the Department of Managed Care, said, quote, not only was this a grave security breach, Kaiser did not actively work to protect patients until after they had been caught. We are imposing this fine because we consider this act to be irresponsible and negligent at the expense—at the time—at the expense of the member's privacy and peace of mind. At the time, the $200,000 fine was the largest the State of California had ever imposed on a health insurer for a breach of patient confidentiality.

This privacy breach occurred as Kaiser was in the early stages of the creation of KP Health Connect. It is the electronic medical records system that you referenced in your testimony, Mr. Ferguson. Has Kaiser had a breach of its patients' personal information since the 2005 breach?

Mr. FERGUSON. Thank you for the question. I don't know of any breach.

Mr. MARKEY. So you are saying they have not had any breaches since then?

Mr. FERGUSON. I don't know of any.

Mr. MARKEY. But you should know. Don't you think you should know? That is the point. That is the point. We need to have security mandated. What specific privacy and security safeguards has Kaiser implemented since the breach to ensure that it doesn't happen again?

Mr. FERGUSON. We have had a very extensive security program in the—implemented through the IT area, including a large program of encryption, including encryption of laptops and endpoint devices. So we have taken this very seriously.

Mr. MARKEY. So would you mind if we built mandatory privacy regulations into this health IT bill? Would you mind at Kaiser?

Mr. FERGUSON. I think this is a complex area.

Mr. MARKEY. But we need strong privacy laws to accompany this, yes or no? I am going to ask the question. Yes or no, should this law as we are passing have strong privacy laws? And it will start down here. Yes or no? Yes, or no, privacy should be included in the health IT bill, strong privacy protections?

Dr. STACK. Appropriate rules, yes.

Mr. MARKEY. Yes. OK. Yes, sir.

Dr. THAMES. Same answer. Appropriate rules, yes.

Mr. MARKEY. OK. Yes, ma'am. Privacy in this bill——

Ms. DARE. Appropriate rules, yes.

Mr. MARKEY. Appropriate rules. What does appropriate mean?

Mr. PALLONE. Mr. Markey, you can keep going with the panel, but you are a minute over. So let them just finish and then we will move on.

Mr. REED. I would say we should have Federal rules in the bill.

Mr. MARKEY. OK. Federal rules. Yes, sir.

Mr. FERGUSON. Appropriate and consistent rules.

Dr. PEEL. Yes, appropriate and consistent rules based on medical ethics and the history of law in this country.

Mr. MARKEY. Thank you.

Ms. MCGRAW. I was going to say ditto, but I don't think I can. Yes, appropriate rules, absolutely.

Mr. MARKEY. Thank you, Mr. Chairman. I appreciate your indulgence.

Mr. PALLONE. You are welcome. Then we are all done. Listen, thank you all very much for being here. We appreciate your input. It was very helpful in terms of moving forward with this discussion draft. And we appreciate your being here.

Next panel, if you would come forward, please. I should mention, as I think I did before, that we may give you some questions to answer within the next 10 days in writing. The second panel, please come forward. Let me welcome our second panel, which I understand consists of one witness, which is Dr. Carolyn M. Clancy, who is Director of the Agency for Healthcare Research and Quality of the Department of Health and Human Services. My understanding is that Susan D. McAndrew—Ms. McAndrew is here to assist you with questions, but not give an opening statement. Ms. McAndrew is Deputy Director for Health Information Privacy of the Office for Civil Rights at the Department of Health and Human Services.

And I think you know the rules: 5-minute opening statement, they become a part of the record, and we may ask you additional

questions to follow up in writing. So thank you, Dr. Clancy. If you would begin.

STATEMENT OF CAROLYN M. CLANCY, M.D., DIRECTOR, AGENCY FOR HEALTHCARE RESEARCH AND QUALITY, DEPARTMENT OF HEALTH AND HUMAN SERVICES; ACCOMPANIED BY SUSAN D. McANDREW, J.D., DEPUTY DIRECTOR FOR HEALTH INFORMATION PRIVACY, OFFICE FOR CIVIL RIGHTS, DEPARTMENT OF HEALTH AND HUMAN SERVICES

Dr. CLANCY. Thank you, Chairman Pallone, Ranking Member Deal and members of the subcommittee. Good afternoon. I am Dr. Carolyn Clancy, Director of the Agency for Healthcare Research and Quality and Operating Division of HSS, otherwise known as AHRQ. And you just introduced Ms. McAndrew for me. And I ask that our written statement be made part of the official record.

Health IT, as you have been hearing from the first panel, is a critically important tool to improve the quality, safety and value of health care. Health IT can help save lives by identifying certain medical errors in realtime, improve quality and efficiency, give health care professionals more advanced decisionmaking tools, and provide individuals with new ways to participate in their care or the care of their loved ones.

To that end, AHRQ has invested $260 million since 2004 to support and stimulate investment in health IT. This translates to almost 200 projects in 48 States. And at the direction of Congress, we have committed a significant proportion of that to rural and underserved settings. However, hardware and software in every health care facility in America alone will not improve quality, safety and value. We need a network that allows for the safe and secure sharing of information in realtime, standards that make the sharing of that information possible, and widespread adoption of health IT by health care providers.

So the catalyst for the creation of the networking standards is the Office of the National Coordinator for Health IT, fondly known as ONC. ONC works to promote the adoption of health IT in American health care. So the analogy here—now that the woman from Verizon has left—is, if everyone had a cell phone but there were no network to plug into, it would be a limited utility. So as you know, health IT has been one of Secretary Leavitt's highest priorities since he took office. His central focus is the adoption and use of standards that allow for the efficient, confidential and timely movement of data and information through the health IT network. He has always maintained that the best way to do this is through a deliberative, transparent and inclusive process that combines the power of government with private sector resources and innovation.

So in 2005, Secretary Leavitt chartered the American Health Information Community, or AHIC, to make recommendations on how to accelerate the development and adoption of interoperable health IT. The AHIC has been an overwhelming success to date. It has provided the venue to set priorities and advance other meaningful recommendations to realize the adoption of standards, to enable interoperable health IT. As an advisory committee, however, the AHIC can take the Nation only so far. It can only make rec-

ommendations to HHS. It cannot take direct action or make decisions that obligate all key stakeholders to follow.

For nearly a year then, the AHIC and HHS have held ongoing public discussions regarding the best possible successor to the AHIC in the form of a neutral independent body that is not controlled, formed by, or required to report to any branch of government. Today is the third and final planning meeting for the AHIC successor at which groups comprised of consumers, physicians, health industry leaders, Federal leaders, and technical experts are presenting their recommendations to implement a sustainable public-private partnership that accelerates and builds on current progress. Our colleague, Dr. Rob Kolodner, the National Coordinator for Health IT, is representing HSS at that meeting, which is why he couldn't join us for today's hearing.

Let me just say that I have been extremely impressed by how many people have stepped forward to volunteer. The new self-governing AHIC successor, wildly inclusive of all stakeholders, will build on the momentum generated by the predecessors and Secretary Leavitt. So in a nutshell, the AHIC to date has translated 30 years of research on health IT and existing standards into tools that improve the quality and safety of health care and it has succeeded because of the involvement of health industry leaders combined with broad engagement of technical experts through working groups. We have made great progress in creating common standards, a process known as harmonizing. And through Secretary Leavitt's leadership and formal recognition, we now have identified many of the most important standards that need to be used for interoperable health records and personal health records.

So I would like to close with just three brief observations regarding health IT and improvement in health care. The first is that health IT is essential to high quality, high value health care, but it is not sufficient. In fact—and you heard this from the first panel—without attention to work flow and processes, health IT can actually speed up mistakes. This was seen in an intensive care unit in a children's hospital in Pittsburgh where the system was implemented very rapidly. So the new electronic system actually exacerbated underlying communication and work flow problems. Thankfully these have since been corrected.

The second is that there are huge opportunities for health IT to transform health care organizations, those that provide care, to contribute to a learning health care system. Health IT can actually help clinicians and patients ensure that they have got evidence that they need when they are making decisions at their finger tips. And it can also enhance much needed language between health care delivery and biomedical science.

And the third point is that clinicians and health care organizations providing care to rural and underserved communities may need additional assistance to improve health care through the effective use of health IT. That has been a big focus for the national resource center that AHRQ supports and one that is certainly worthy of continued attention.

So let me close by saying that we look forward to working with the Committee on our shared commitment to health IT and improved health care in discussing the implications of adopting

health IT standards and certification criteria through rulemaking. Our concern derives from prior statutory requirements in environments where standards evolve at a rapid pace, and the concern is that the rulemaking has the potential to chill progress and prevent interoperability rather than promote it.

So thank you for your time, and I very much look forward to your questions.

[The prepared statement of Dr. Clancy follows:]

Testimony

Before the Subcommittee on Health of the Committee on Energy and Commerce

U.S. House of Representatives

Statement of

Carolyn M. Clancy, M.D.
Director, Agency for Healthcare Research and Quality
U.S. Department of Health and Human Services

For Release on Delivery
Expected at 10:00 a.m.
Wednesday, June 4, 2008

Chairman Pallone, Ranking Member Deal, and Members of the Subcommittee, thank you for inviting us here today to present the Administration's views on draft health information technology legislation. I am Dr. Carolyn Clancy, Director, Agency for Health Care Research and Quality (AHRQ) and I have with me today Ms. Sue McAndrew, Deputy Director for Health Information Privacy, HHS Office of Civil Rights. Additionally, I will be speaking on behalf of the Office of the National Coordinator for Health IT. Dr. Kolodner is currently attending scheduled meeting of the American Health Information Community successor stakeholders. As you know, efforts to ensure availability of interoperable health information technology are one of the Secretary's highest priorities. We appreciate your dedication to health information technology and share your commitment to this important issue.

Efforts To Date

Office of the National Coordinator for Health IT (ONC)

On April 27, 2004, the President signed Executive Order 13335 supporting the promotion of health information technology (health IT) to improve efficiency, reduce medical errors, improve quality of care, and provide better information for patients and physicians. The President also called for most Americans to have access to secure, interoperable electronic health records (EHRs) by 2014 so that health information will follow patients throughout their care in a seamless and secure manner. As part of this, the President directed HHS to establish the position of the National Coordinator for Health Information Technology.

In further support of this goal, on August 22, 2006, the President issued Executive Order 13410 to ensure that federal agencies that administer or sponsor a federal health care programs (as defined by the Order) promote quality and efficient delivery of health care through the use of

interoperable health IT, transparency regarding health care quality and price, and better incentives for program beneficiaries, enrollees, and providers. Executive Order 13410 directs that "[a]s each agency implements, acquires, or upgrades health information technology systems used for the direct exchange of health information between agencies and with non-Federal entities, it shall utilize, where available, health information technology systems and products that meet recognized interoperability standards."

ONC has helped lead in a number of key areas. As part of this, yesterday, ONC released the Federal Health IT Strategic Plan. This 5-year Federal strategic plan is necessary to achieve the nationwide implementation of a health IT infrastructure.

American Health Information Community (AHIC)

The development of common standards, and a process to certify products and services as meeting those standards, is a key priority. Secretary Leavitt chartered the American Health Information Community (AHIC) as a Federal Advisory Committee to make recommendations on how to accelerate the development and adoption of interoperable health IT. The AHIC has provided the venue to make recommendations to the Secretary on priorities and has advanced other meaningful recommendations to realize the adoption of health IT. Health-related priorities recommended by the AHIC enable the identification of health IT standards by the Healthcare IT Standards Panel (HITSP) and certification of health IT products by the Certification Commission for Healthcare IT (CCHIT)

While HHS and the Federal government play pivotal roles in the health care system and in its forward progress, public and private stakeholders must also be aligned to rapidly and effectively achieve this interoperability. Therefore, the AHIC and HHS have had ongoing

discussions regarding the best possible successor to the AHIC, including discussions of the successor entity's role, funding, and governance structure. It is envisioned that the AHIC successor will be an independent and sustainable organization that will bring together the best attributes and resources of public and private entities, a public-private partnership. Such an entity must be a neutral, independent body that is not controlled by, formed by, or required to report to any branch of government.

LMI Government Consulting, assisted by The Engelberg Center for Health Care Reform at the Brookings Institution and working under a cooperative agreement with the HHS is convening stakeholders to create a nationwide focal point for health information interoperability as a public-private partnership. The goal is an orderly transition that will accelerate nationwide initiatives aimed at using information technology to enable improvements in the quality and efficiency of health care in the United States. In fact, the third AHIC Successor meeting is taking place today from 9 a.m. to 12 noon. During this meeting, recommendations from the Planning Groups for the AHIC Successor will be announced.

Standards & Certification

In fall 2005, HHS worked with the American National Standards Institute (ANSI) to form a public-private collaborative, known as the Healthcare Information Technology Standards Panel (HITSP), to harmonize existing health IT standards, and to identify and establish standards to fill any gaps in those existing standards. Experts from approximately 500 health care related organizations participate in HITSP and engage in a consensus-based process to harmonize relevant standards in the health care industry and to ensure that there is detailed guidance on how the standards need to be used. This process enables and advances interoperability of health care

applications, and helps ensure that health data supporting the delivery of care will be accurate, exchangeable, private and secure.

We have now identified many of the most important standards that need to be used for interoperable electronic health records (EHRs) and personal health records. To date, the Secretary has recognized 52 harmonized standards, and he will recognize 60 new harmonized standards in January 2009. Under Executive Order 13410, Federal agencies that administer or sponsor a Federal health care program (as defined in the Executive Order) are expected to utilize, where available, the health information technology systems and products that meet recognized interoperability when they implement, acquire, or upgrade health IT systems for the direct exchange of health information between agencies and with non-Federal entities. Those agencies are also expected to require in contracts or agreements with health care providers, health plans, or health insurance issuers that as each provider, plan, or issuer implements, acquires, or upgrades health information technology systems, it utilizes, where available, health information technology systems and products that meet recognized interoperability standards.

In the private sector, the Certification Commission for Healthcare Information Technology (CCHIT) will be certifying products that use recognized standards during its next cycle which begins this July.

Providers and consumers must have confidence that the electronic health information products and systems they use can perform a set of well-defined functions, are secure, can maintain data confidentiality as directed by patients and consumers, and can work with other systems to share information. CCHIT currently certifies both ambulatory and inpatient EHRs, and has also begun developing a certification processes for health information networks and specific components of PHRs. Through its public-private process, CCHIT develops specific

certification criteria for health IT systems and then rigorously evaluates them to determine that they truly meet criteria for functionality, security and interoperability. After just two years, over 150 EHR products have been certified. These certified products now include over one third of the enterprise EHRs and, adjusting for market share, over 75% of the ambulatory EHRs being sold in the US today.

Nationwide Health Information Network

To support the goal of an interoperable network, there are presently sixteen separate trial implementations of the Nationwide Health Information Network (NHIN) Cooperative. The NHIN Cooperative involves public and private health information exchange organizations across the country that can move health-related data among entities within a state, a region or a non-geographic participant group. The NHIN is a "network of networks." Our goal is to eliminate all of the obstacles to advancing the NHIN into a production-ready state by the end of this calendar year. To do so, the NHIN will need to demonstrate technical readiness with on-site, interoperable and secure health information exchange based on common specifications. Four core services will be included: 1) delivery of data, including a summary patient record, across the involved health information exchanges; 2) the ability to look up and retrieve data across the exchanges from EHRs and PHRs; 3) the ability for consumers to express preferences about whether and how, they will allow the electronic exchange of their data; and 4) supporting the delivery of data for our nation's health uses, such as public health and emergency response.

Collaboration with NIST

In order to achieve interoperability and allow health care organizations to securely connect to each other, there must be rigorous testing of detailed data and technical standards. This testing requires testing tools and expertise that ensure that each participating organization and software system is exactly meeting these standards. Toward this goal, the ONC has been working with the National Institute of Standards and Technology (NIST) to advance testing architecture nationally. This work involves developing conformance testing capabilities and the use of testing to ensure that standards are adequate, that the standards are properly implemented in systems and, as a result, that the systems can interoperate. NIST has helped with the HITSP harmonization process and with CCHIT's initiation of conformance testing capabilities. NIST is also helping with the rigorous testing activities necessary to support the NHIN and have a secure, interoperable network of networks operating on top of the public Internet.

Privacy

HHS recognizes that there are important issues relating to the protection of information in an electronic health information exchange environment. Maintaining the privacy and security of information shared through the electronic exchange of health information is paramount. We believe that the use of health IT in accordance with appropriate polices can protect private information more successfully than can be done with paper records , can make it easier for individuals and their doctors to access and share health information, and can improve care coordination. Just as it was a core value underpinning the enactment of HIPAA in 1996, so too today, privacy is critical to the success of our new nationwide, interoperable health IT vision.

The *Standards for Privacy of Individually Identifiable Health Information* – better known as the HIPAA Privacy Rule have been in operation for the past five years, and have proven their

workability and adaptability for the broad range of health plans and health care providers charged with keeping health information secure and confidential. HHS' Office for Civil Rights (OCR) has a solid record of enforcement of these standards, having brought about significant and systemic improvements in compliance by over 6,100 covered entities as a result of its investigations and the voluntary compliance efforts of the entities.

The Privacy Rule is carefully balanced to ensure strong privacy protections without impeding the flow of information necessary to provide access to quality health care. To that end, the Rule permits covered entities to share protected health information for core purposes – to treat the individual, to obtain payment for the health care service provided, and for health care operations – without obtaining the individual's prior authorization. The Privacy Rule also permits other uses and disclosures of protected health information without an individual's authorization, including those disclosures necessary for a limited number of public interest disclosures, such as for public health purposes. Additionally, of course, the individual may authorize in writing any other use or disclosure of protected health information, and must do so before a covered entity may use or disclose such information to market the goods or services of another to the individual. These protections apply to protected health information whether in paper or electronic form, and thus have proven effective in protecting information in electronic health record systems in existence today.

The HIPAA Privacy and Security Rules will also serve as an effective baseline of protections as we begin to transform health care through the use of healthIT and the electronic exchange of information through secure interoperable, interconnected networks. A privacy and security framework for the exchange of electronic health information built on the foundation of HIPAA, permits us to explore the enormous potential of health IT to bring new opportunities for

consumer participation in and choices about their own healthcare, while effectively identifying and addressing new risks to privacy and new opportunities to secure health information. Together with public input through several advisory bodies, the Department is actively examining these issues. For example, healthIT can make it easier and faster to effectuate the individual's rights under HIPAA to access and get a copy of their medical record, to have that record amended if it is incomplete or incorrect, and to know about certain disclosures of their information. We are equally concerned with the potential risks to privacy as a result of the easier flow of information through health IT. As the roles of vendors and service providers in the NHIN evolves, we will need to ensure that a privacy and security framework that guides their responsibilities and obligations to consumers, without unduly restraining the development or adoption of health IT.

Linking Quality and Health IT

The intersection between research and the application of how new knowledge is applied to improve care is the Agency for Healthcare Research and Quality's (AHRQ) unique contribution to the health IT enterprise. Accordingly, the AHRQ Health IT program explicitly researches how health IT tools can improve the quality of health care, while ONC focuses on advancing the adoption and interoperability of health IT.

Since 2004, AHRQ has invested $260 million to support and stimulate investment in health IT. This translates to almost 200 projects in 48 States, many of which projects have been focused towards rural and underserved populations.

AHRQ-funded projects cover a broad range of health IT tools and systems, including electronic health records, personal health records (a term that specifically denotes health

information collected by and under the control of the patient), health information exchange, electronic prescribing, privacy and security, clinical decision support, quality measurement, patient-centered care, provider workflow, and Medicaid technical assistance.

AHRQ created the publicly available, online National Resource Center for Health IT (the Resource Center) to disseminate research findings, lessons learned, and case studies on the implementation and impact of AHRQ-funded health IT projects. The Resource Center leverages our investments in health IT by offering help where it is needed—real world clinical settings that may feel ill equipped to meet the implementation challenge—facilitating expert and peer-to-peer collaborative learning and fostering the growth of online communities who are planning, implementing, and researching health IT.

AHRQ collaborates with ONC and others to assure that our investments are closely aligned and concentrate specifically on the use of health IT to improve safety and quality in diverse health care settings.

To ensure that we harness the power that health IT has to offer, we need to develop an evidence-based strategy to help clinicians and health care leaders decide which health IT innovations should be adopted and how they should be implemented to maximize value—both to clinicians and patients today and to the public health and research enterprises.

HHS VIEWS OF DISCUSSION DRAFT HEALTH IT BILL

We appreciate the opportunity to provide initial comments on the discussion draft. We have been working with the Committee staff on the discussion draft and providing technical assistance. For purposes of this testimony, we will therefore take this important opportunity to discuss only the high-level issues we have with the proposed discussion draft.

Proposed Health IT Federal Advisory Committees (FACA)

The discussion draft would establish in statute two separate Federal advisory committees- an HIT Policy Committee and an HIT Standards Committee. We have significant concerns about freezing a particular set of structures in statute. In 2005, Secretary Leavitt chartered the American Health Information Community (AHIC) as a Federal Advisory Committee to make recommendations on how to accelerate the development and adoption of interoperable health information technology. For nearly a year, the AHIC and HHS have had ongoing discussions regarding the best possible successor to the AHIC, including discussions about its role, funding, and governance structure. It is envisioned that the AHIC successor will be an independent and sustainable organization that will bring together the best attributes and resources of public and private entities, a public-private partnership. Such an entity must be a neutral, independent body that is not controlled by, formed by, or required to report to any branch of government in order to assure independence and continue to build on progress to date.

The creation of new advisory committees under this bill would significantly interfere with the progress made in establishing an AHIC successor thus far. This approach would preempt and discount the significant efforts made by stakeholders to establish the AHIC successor, and impede efforts to foster the adoption of health information technologies and standards and realize an interoperable nationwide health information system.

Additionally, the proposed advisory committees' membership would be determined through a political appointment process. We are concerned that the membership of these FACAs would politicize the successful collaborative advisory work ongoing through AHIC and the collaborative work going on through the current conveners of the AHIC Successor and would

create barriers to rapid progress. Additionally maintaining two organizations could prove duplicative and costly.

Accordingly, we encourage the Committee to strike proposed sections 3002 and 3003 and allow the current public-private collaborative process already underway to proceed.

Proposed Process to Develop and Recommend Standards, Implementation Specifications and Certification Criterion

The discussion draft proposed to establish a FACA advisory committee known as the HIT Standards Committee, to recommend standards, implementation specifications and certification criteria to ONC for endorsement. Upon ONC endorsement, the recommendations would be sent forward to the Secretary for adoption through a Federal rulemaking process.

The adoption of health IT standards, implementation specifications, and certification criteria through the use of rulemaking should be avoided. We have seen from prior statutory requirements that it significantly delays the applicability and usage of new and improved standards.

Proposed Privacy and Security Provisions

Business Associate Provisions

The Discussion Draft has three separate provisions relating to Business Associates. Section 316would state that organizations that require access to protected health information and transmit it to a covered entity, such as Health Information Exchanges, Regional Health Information Organizations (RHIO), and those involved in e-prescribing, must be treated as business associates for purposes of section 311. Section 311, in turn, would limit the use or

disclosure of protected health information by a business associate to the purposes specified in the contract with the covered entity and would subject the business associate to civil and criminal penalties under HIPAA for violation of such contract terms. Similarly, section 301 would apply administrative, physical, and technical security standards to business associates and would also apply the HIPAA civil and criminal sanctions to a business associate for violations of these standards.

Under current law, only covered entities are subject to liability for violations of the HIPAA Privacy and Security standards. Business associates, because they are not covered entities, are therefore not liable for violations, through the covered entities themselves may, in some circumstances, be liable for the violations by their business associates. Under the Discussion Draft, RHIOs, Health Information Exchanges (HIE), and similar organizations, would still not become covered entities under HIPAA, but they would become liable for HIPAA civil and criminal penalties for using or disclosing protected information in a manner contrary to the terms of their business associate agreements with covered entities. While this is one approach to address gaps in the current coverage of HIPAA, the provision would not result in evenhanded treatment as other entities, such as PHR vendors, are not encompassed in this solution.

Moreover, in extending liability to business associates, the Discussion Draft would sweep all business associates under this same provision, making them all liable for contract violations. The potential exposure to criminal and civil liability may chill many from becoming business associates or may raise the cost of doing business in this manner. Many business associates (for example, interpreters) help consumers and others such as transcription services or accreditation services are essential for routine business operations.

Proposed Grants and Loans

Section 3011 of the discussion draft would provide for competitive grants and loans to facilitate the adoption of qualified health IT. The Administration does not believe that grants (or grant-supported state loan programs) are the most efficient manner to stimulate the widespread adoption of health IT; it believes the most appropriate and efficient ways to achieve widespread use of health IT are through market forces, rather than through direct subsidization of health IT purchases. In August 2006, the Centers for Medicare &Medicaid Services (CMS) and the Office of the Inspector General (OIG) promulgated two final rules with an exception to the physician self-referral prohibition and a safe harbor under the anti-kickback statute, respectively, for certain arrangements involving the donation of interoperable EHR technology to physicians and other health care practitioners or entities from businesses with whom they work. The exception and safe harbor have made it possible for physicians and other health care practitioners or entities to obtain EHR software or information technology and training at substantially lower prices, up to 85% below the market costs.

Other Comments on the Discussion Draft

The discussion draft codifies the Office of the National Coordinator for Health Information Technology. The Administration does not support statutorily establishing individual offices, which can limit needed flexibility to adjust duties and responsibilities as time requires.

The Administration continues to review this bill and anticipates having additional comments and questions about its impact and certain provisions. As part of this we are carefully reviewing

sections 111 and 112 to assess and understand their potential impact on Federal programs, including Medicare, and the private sector. We are also carefully reviewing sections 302 and 315, regarding notification of breach of privacy, and section 312, to assess its impact on adoption of health IT.

CONCLUSION

The Administration shares the goals of the Committee with respect to health IT and looks forward to continuing work with you to improve the quality of our nation's health care through its use. We hope to continue our work with the Committee as we move forward to address these concerns.

Mr. PALLONE. Thank you, Dr. Clancy. And I will start with the questions. In 2006, the President issued an Executive order that requires—and I quote—as each agency implements, acquires, or upgrades health information technology systems used for the direct exchange of health information between agencies and with non-Federal entities, it shall utilize where available health information technology systems and products that meet recognized interoperability standards or standards that allow for the electronic communication of health information among providers, insurers, and others. In addition, it says—and I quote—each agency shall require in contracts or agreements with health care providers, health plans, or health insurance issuers, that as each provider plan or issuer implements, acquires or upgrades health information technology systems, it shall utilize where available health information technology systems and products that meet recognized interoperability standards.

That is a mouthful. I just wanted to ask you. Can you tell us how this Executive order is being currently applied? And then I wanted to mention a few other things about who it applies to. But how is it being currently applied?

Dr. CLANCY. Sure. Let me give you two pieces of information. One, there is a scorecard process. As you might imagine, the trick here is for those programs like Veterans Affairs that are owned and controlled by the Federal Government, it is a different sort of process than the military treatment facilities for that matter. They have the direct control to make that happen rapidly. When you are talking about a contracting process, it takes a little bit more time. There is a scorecard process which gets reported to the Office of Management and Budget, and we would be happy to provide more detailed follow-up information on the status of that scorecard.

Mr. PALLONE. If you would, I would appreciate it.

Dr. CLANCY. The second piece I would add about the Executive order is we all see that there is a huge opportunity for health IT to support improvements in quality and safety and care. Right now. most commercially available products actually do not enable you to report on quality electronically. You can't just sort of hit F7 and up go the quality measures. But that has been a very clear focus of a current AHIC Quality Work Group that I co-chair.

Mr. PALLONE. If I could just get a yes or no because I want to get to a second question as to where this Executive order applies. Does it apply to plans under the Federal employee health benefits?

Dr. CLANCY. Yes.

Mr. PALLONE. Does it apply to Medicare fiscal intermediaries?

Dr. CLANCY. Yes.

Mr. PALLONE. And does it apply to Medicare Part D plans?

Dr. CLANCY. I believe so, but I would have to follow up with you.

Mr. PALLONE. If you would get back to us. And it does it apply to Medicare Advantage plans?

Dr. CLANCY. Yes.

Mr. PALLONE. And finally, does it apply to providers through the Medicare conditions of participation?

Dr. CLANCY. I don't believe it is framed as a condition of participation. It is framed as what we would do under contracting mechanisms.

Mr. PALLONE. OK. If you would get back to us in writing on the other.

The second question—you have testified that HHS seeks to fully privatize the American Health Information Community, or AHIC, which currently exists as a Federal advisory committee to find and make recommendations on the future direction for HIT. And the private entity is required to be self-sustaining financially. So I am fearful, as I mentioned before, it could be based on a pay-to-play model. I have concerns with maintaining a strong beneficiary and consumer voice and ensuring transparency in the process of developing policies and standards for the electronic exchange of health information. A committee pursuant to the Federal Advisory Committee Act, FACA, has transparency and notice requirements that allow for strong consumer involvement and transparency. For example, FACA requires timely notice of each public meeting through the Federal Register. It requires the committee to permit interested persons to attend its meetings, to appear before the committee and to submit written statements with the committee. It requires that detailed minutes be maintained and that all committee minutes transferred for board studies and more be available for public inspection and copying.

On the other hand, a fully private entity could settle on a pay-to-play model since it has to be financially self-sustaining. Vendors, employers and others have more money that can enable them more votes or a louder voice. It can make decisions in a nonpublic meeting without input from all interested parties.

You get the drift of what I am trying to contrast here. So I have one issue. Do you disagree with ensuring a strong public and consumer voice through these requirements guaranteeing a public, open, and transparent process? I mean, what is going to happen here if this isn't fully private?

Dr. CLANCY. Sir, Secretary Leavitt believes very strongly and has always maintained that the best way to make progress is to have a process that engages the most senior decision makers in the public and private sectors and brings with that representation from all stakeholders that is broadly inclusive. I don't think transparency and the notion of broad inclusivity has to be limited to a FACA process. I would say that our biggest concern is actually loss of momentum from the AHIC that is operating now to setting up a new FACA. But I am describing for you what our concerns are.

Mr. PALLONE. But do you share my concerns that we might enter into this pay-to-play model and not have this transparency?

Dr. CLANCY. As envisioned, the AHIC successor won't be successful. It won't succeed, and it won't engage the Federal Government as a major participant as we are committed to do right now unless it does have that kind of representation. And I think the big question is how do you build on the momentum that exists right now and engage broad participation? That, I think, is the real question, and our proposal is this succession process which has already been in play for most of the past year.

Mr. PALLONE. But you really haven't addressed my concerns. How are you going to address those?

Dr. CLANCY. It is going to need to be a requirement, and I think the Federal Government will have to make their condition of en-

gagement with this activity contingent on making sure the consumers are heard from. That has been a very, very high priority for us; how to get to a sustainable business model is an interesting question. But I think that we are committed to paying our fair share as part of that business model moving forward. I don't think I have seen a number of multi-stakeholder collaborative processes where they do have transparency, where they do let people know about meetings and so forth. So I don't think that has to necessarily come under a FACA.

Mr. PALLONE. So you would try to build those provisions in?

Dr. CLANCY. Yes.

Mr. PALLONE. OK. Thank you.

Mr. Deal.

Mr. DEAL. As I understand it, you believe that a public/private partnership is preferable as to a successor to AHIC rather than the formulation set forth in this draft legislation; is that correct?

Dr. CLANCY. Yes.

Mr. DEAL. Would you elaborate on why you think that is preferable?

Dr. CLANCY. I think the one concern is loss of momentum. This succession process has been in place, got started almost a year ago, and for the past 4 months or so what we have put in motion through a convening process is a grant to the Engelberg Center at the Brookings Institution working with another contractor in McLean, Virginia, LMI, to put in place a very elaborate planning process. They have engaged very senior leaders in health care, physicians, hospitals, health care organizations and so forth, as well as very broad representation from stakeholders. And I have been enormously impressed by every place that I speak or interact with folks that are in health care how many people are engaged in very much following this process. So that level of engagement, I think, is going to be necessary to make this enterprise move forward in a way that we all want.

So I would be worried about loss of momentum, and as I said to the Chairman, I don't think that transparency and a strategy that assures that ability to pay is not the condition for participation has to be limited to a FACA, so that would be our concern.

The last comment I would make is through our work with the AHIC and work groups and so forth, I have been enormously impressed by how many people have stepped forward in a voluntary way through the work group process. And I have also been impressed that to make progress, you need to bring together people who are users; that is to say who are affected, whether it is clinicians putting this in their practices, or their patients worried about what happens to my information. You need people who understand policy, and you need people who really understand the technical details, the kinds of details that we all want to say, give me the bottom line here. But they are incredibly important, and what you need is a process that can actually pull all that together, and then you need decisionmakers who say, OK, we are going to move with this. And Secretary Leavitt believes that the sustainability of a public/private process that is docked in the private sector is most likely to succeed.

Mr. DEAL. In other words, if we ingrain it in statute, we lose a lot of the flexibility and ability to adapt the standards maybe as they should be altered or changed in the future?

Dr. CLANCY. That is one concern, yes. The second is that the appointments process inevitably has some risk of politicization, a word I can't say very easily.

Mr. DEAL. As I understand from your background, there is a lot to be gained through electronic medical records in the ability to assess overall treatment modules that are used in the health care system, the effectiveness of tests, the effectiveness of various procedures. Would you elaborate on that? Because that is a little bit out of the realm of what we have talked about up to this point.

Dr. CLANCY. Sure. So everyday in health care in the paper world, clinicians and patients make decisions together, and it is sort of scribbled down on paper, and we don't get to learn very much. We don't get to learn very much about the off-label use of medications. For example, a report that we sponsored found that that happens about 20 percent of the time, often very appropriate, it is legal. And there is a lot to learn because when clinicians and patients come to a problem where they don't have any good answers, and they try something new, it would be great to learn from that, and we don't have a way to do that.

If you have interoperable records, you have a strategy to be able to learn that. Similarly, you have a strategy where right now if I am seeing patients, and I have a patient who might benefit from being in a clinical trial, I have to think, clinical trial, and type in to get to a Web site at NIH, which is a wonderful resource. That could actually be linked with an electronic health record, which already pops up for me the information about which clinical trials the patient is eligible for and so forth. And it becomes the platform to give clinicians information in the same way that Amazon does.

You know, when I logged on to Amazon not too long ago, they let me know that Bruce Springsteen, who I like, had a new CD out, and thankfully did not give me any information about Britney Spears. And so technologically we know how to do that.

The big opportunity for my agencies and others working together, and we are working on this, is to distill knowledge so it, too, can be built into electronic health records, which means that effectively we can shorten the way-too-long time frame we have to translate research findings into practice. That, I think, is going to be a part of the huge promise that you were hearing about in the first panel.

Mr. DEAL. Thank you, Mr. Chairman.

Mr. PALLONE. Thank you, Mr. Deal.

The gentleman from Texas. Mr. Gonzalez.

Mr. GONZALEZ. Thank you very much, and welcome, Dr. Clancy. And I am not sure that you covered it in your statement. Does HHS have a pilot or demonstration project out there right now that will soon be taking effect? I know that I think you are soliciting for participants. I try to get some doctors out of San Antonio, but I think you required a limit of 200 physicians to basically form—I'm not real sure. Are you familiar with what I am making reference?

Dr. CLANCY. We have an EHR, electronic health record, demonstration program that CMS is sponsoring, which is actually going

to be giving physicians incentives to adopt health IT, and then in subsequent years those incentives will be linked to achieving certain quality goals. I am not sure that is what you mean.

Mr. GONZALEZ. My understanding was, again, a demonstration or pilot project. The only thing I was concerned about is you didn't have that many qualified applicants, or you didn't even have that kind of response, because the conditions, as I understood them, and maybe I will just follow up when I get more information, but I know I couldn't get my medical society and the number of doctors to really come together because the numbers were so great, and then only half of these doctors would be eligible for any of the incentives, and then the other half would not, which was a rather curious way of doing it.

My concern is that when we have CMS going out with pilot demonstration projects, then what you glean from that sometimes determines which direction we take, and so the quality of the demonstration process determines the quality of the product. And I hate to say that you all have not been real successful in some of those things, whether it is the medical equipment or the coding system or the racks, and we could go on and on. But nevertheless, I will follow up on it.

The other question that I have, you heard from a representative of Cisco, and she referred to it as market uncertainty. And yet in your testimony—and I think the only way we ever get to market certainty, not uncertainty, is probably through government sponsorship, stewardship. And so I know you have had this discussion with the Chairman, and I know Mr. Deal made reference to it. Mr. Deal indicated that we shouldn't be legislating this.

My understanding is what we are setting up is a regulatory scheme where we actually authorize a governmental entity or agency to study, promulgate rules and so on. It is not necessarily set in stone. It is my understanding, I could be wrong, that we are setting some sort of legislative definition, qualifications, requirements and standards. I don't think we are doing that, so I don't think we are really legislating that.

What we are doing is creating a regulatory scheme which works very well, and I think the only way we probably will provide that type of certainty that the doctors are out there calling for before they make this kind of substantial investment. Wouldn't you agree that that is a sound way of approaching what Ms. Dare characterized as the market uncertainty aspect of it?

Dr. CLANCY. Well, if I think about physicians in Texas, I would guess that many of them are contracting with multiple insurers. That is how the market works in most places, and, in fact, what is driving a lot of physicians, particularly those in small practices, a little bit crazy is the burden of having multiple different requirements for multiple private insurers and CMS.

So ultimately to make progress, I think there has to be an alignment of policy interests and objectives between the public and the private sectors, which means that, in essence, what you need is an entity that promotes a sustainable public/private partnership. So if I am in Texas, I am an internist and I am in internal medicine, and I see, say, a third of my patients are on Medicare, and then two-thirds are accounted for by 8 to 10 private insurers. If they all

have different reporting requirements or different aspects of care that they want me to report on: A, I am probably going to go crazy; B, that doesn't help with my decision about should I buy an electronic health record. If they are asking for common reports about quality of care and have a common approach to incentivizing the adoption of electronic health records, I think that really begins to set the stage.

The key to getting that kind of agreement is having an entity that supports that sort of public-private alignment.

Mr. GONZALEZ. I think this bill would accomplish that in the scheme that we envision, and that some philosophically or for their own ideologies fear that the government is setting standards and requirements which the government has to. It is going to have private involvement, no doubt. I tell you that now.

From the private insurance—and I don't know that we are discussing two different things. If we are talking about what we are going to be adopting in the way of systems, what their capabilities are to make sure that they talk to one another, that we have this interoperability, that is one thing. Now, an insurance company may have their own quirks and such, and they do it for their own reasons. And they are only going to adopt that which HHS or CMS has when it is to their advantage, such as a physician compensation standard and such, but they surely aren't on prompt pay. They surely are not on uniformity of claims and such, and hopefully we will address that in the future because I think they really do game the system to their advantage.

But I am not talking about all that. I am just saying what does the equipment look like? What should be its capabilities? What should be the standards? What should be the minimums so that when doctors make this investment, they know that, looking forward, they are going to have to maintain it? It is going to cost money, as Dr. Stack indicated, but they know it is not going to be obsolete. We have many doctors who have had bad experiences and are really——

Dr. CLANCY. Oh, yes.

Mr. GONZALEZ. I applaud HHS, CMS and Governor Leavitt for their work. But so much more needs to be done, and I would hope that you would embrace this particular concept. We have a lot of legislation out there. This one is probably going to be the most viable and gets us started. We are way, way behind, and this does impact the quality of care for all the patients throughout this country.

Thank you very much, Mr. Chairman.

Mr. PALLONE. Thank you, and thank you, Dr. Clancy.

We didn't hear from Ms. McAndrew, but thank you for being here with us.

I think I mentioned before, and I will remind the Members, that within 10 days, if they have questions in writing, we are supposed to submit them to you. So if we have some of those, the clerk will notify you within the next 10 days.

But again, thank you, and we started out saying this is a discussion draft, and obviously we want to take your input and that of the other witnesses as we proceed over the next few weeks. We would like to do a bill this session, obviously, but we are going consider to continue to take comments, if you will.

Dr. CLANCY. I know straight from him that Secretary Leavitt very much looks forward to working with you on that, so thank you for having us.

Mr. PALLONE. Thank you again, and without objection, this meeting of the subcommittee is adjourned.

[Whereupon, at 1:20 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

STATEMENT OF HON. DIANA DEGETTE

Thank you Mr. Chairman. A number of my colleagues, the Oversight & Investigations Subcommittee, and I took a trip last year to New Orleans to conduct a field hearing on the hospital infrastructure of the city in the aftermath of Hurricane Katrina. Some of the hospitals there were in literal ruins, and thousands and thousands of individual medical records were ruined. In many cases, those files contained the entire medical history of many of the city's residents and represented millions of dollars of tests, diagnosis, and treatment.

At the same time, as soon as power to the city and telecommunications was restored, some pharmacies were able to bring up prescription records with ease. With a nationwide database, customers had access to critical information about their personal health, both in New Orleans and in the cities to which they had relocated. We need to have a system of health information that makes this specific experience with Hurricane Katrina the norm, not the experience faced by the patients of Charity Hospital and other health care providers.

That trip reinforced my conviction that health information technology is an absolutely vital piece of the health care puzzle and a direction we need to move in with greater haste.

Mr. Chairman, I sincerely believe that adoption of health information technology, particularly electronic health records (EHRs), will have a profound impact on our health care system. Using electronic prescribing, these problems will be eliminated as pharmacists will clearly see the prescription and be able to cross reference that with the patient's EHR to identify possible drug interaction problems. Billing will also be drastically improved as standardized forms make it easier for claims to be processed by Medicare, Medicaid, and private payers.

And in fact we've already seen tremendous progress with electronic health records in many regards, for example the Veterans Affairs system.

Now, having said all that, we must not fool ourselves into thinking that health information technology, in and of itself is a panacea for all the problems of our health care system. Moving to a more electronically-based system brings its own set of challenges, primary among them, the issue of privacy. And privacy is a big issue indeed.

The Federal Government's record on safeguarding the privacy of sensitive personal information is marred by troubling lapses. In 2006, for example, personal information on 26 million veterans, including their Social Security numbers and birth dates, was stolen from the home of a Department of Veterans Affairs. The employee had taken the data home without authorization.

In another troubling incident, a laptop computer containing medical records of 2,500 patients enrolled in a National Institutes of Health study was stolen from the trunk of a researcher's car. The patients' records were not encrypted, in violation of federal security policies. NIH waited nearly a month before sending letters to notify the patients.

A viable health IT system must include safeguards to protect patients from privacy breaches like these.

Having been a member of this committee for almost 12 years now, I can remember the many debates on privacy we have had in the context of other issues, such as financial services. Ah, the good old days when those issues were under our jurisdiction. We had some very productive debates about privacy when we worked on financial services reform, electronic signatures etc., and much of what we debated and learned during those hearings are relevant today as we discuss privacy in the health care realm.

However, I also want to draw attention to the benefits that can come from strengthening of our Nations' health IT systems. Denver Health and Hospital System, in my district, has a revolutionary health IT system that allows for interoperability and access at numerous providers across the city. Although their system is still in its early stages, with many components that still need to be added, it has drastically improved the health of many Denver residents. Currently, patient

records are scanned and electronically available to all providers at the main public hospital emergency room, at the many community health centers across the entire city, at the school health centers located within the schools, as well as at other providers with the Denver Health and Hospital System.

So, if a child goes to the emergency room late one night and then presents at the school health clinic or a even a community health center, the doctors and nurses instantly have knowledge about previous visits to the ER, any tests that were done, medicine that was given, etc., even if the child neglects to tell the doctors about those visits. This saves tremendous amounts of money on duplicate tests and improperly managed conditions. It also leads to greatly improved health outcomes through coordinated care and better management of chronic health conditions.

Although it is not yet a fully interoperable electronic health record (EHR), I think the Denver Health system shows us the potential benefits that can come of health IT and why it is so important that we pursue a coordinated, interoperable health IT system with nationwide standards and adequate privacy protections.

June 2, 2008

The Honorable John D. Dingell
Chairman
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Joe Barton
Ranking Member
Committee on Energy and Commerce
2322A Rayburn House Office Building
Washington, D.C. 20515

The Honorable Frank Pallone, Jr.
Chairman
Subcommittee on Health
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Nathan Deal
Ranking Member
Subcommittee on Health
2322A Rayburn House Office Building
Washington, D.C. 20515

Dear Bipartisan Leaders:

On behalf of the 53 million Americans represented by Divided We Fail, we urge you to approve Health Information Technology (HIT) legislation this year to spur adoption of a nationwide interoperable HIT system and prioritize the allocation of funds for a secure, interoperable, HIT infrastructure.

Divided We Fail – comprised of AARP, Business Roundtable, Service Employees International Union (SEIU) and National Federation of Independent Business (NFIB) – is an effort to break the partisan gridlock to improve health care and long-term financial security for all Americans.

HIT legislation is critically important to improving our health care system. The health care industry will increase their investments in and deployment of HIT, if Congress acts to:

- Establish a public-private process to set standards;
- Offer financial incentives to encourage the adoption of HIT;
- Educate Americans on the value of electronic health records and information on quality of providers; and
- Address privacy and security questions.

We are pleased that your recently released draft legislation is designed to strengthen the quality of health care, reduce medical errors and costs by encouraging the adoption of HIT. This thoughtful, bipartisan efforts marks real progress toward our goal of enacting HIT legislation this year. Virtually every other sector of our economy has embraced the transformative power of technology. Doing so in health care will improve the safety and delivery of health care.

We look forward to working with you and the Committee to pass HIT legislation that can be signed into law by the President this summer.

Sincerely,

Divided We Fail

cc: Rep. Charles A. Gonzalez
Rep. Bart Gordon
Rep. Phil Gingrey
Rep. Anna Eshoo
Rep. Michael J. Rogers
Rep. Edward J. Markey
Rep. Rahm Emanuel
Rep. Lois Capps
Rep. Edolphus Towns

eHEALTH INITIATIVE
Real Solutions. Better Health.

Statement of Janet M. Marchibroda
Chief Executive Officer
eHealth Initiative and eHealth Initiative Foundation

Before the

U.S. House of Representatives
Committee on Energy and Commerce
Subcommittee on Health

June 4, 2008

818 Connecticut Avenue, N.W, Suite 500 Washington, D.C. 20006 Tel: 202.624-3270
www.ehealthinitiative.org

U.S. House of Representatives
Committee on Energy and Commerce, Subcommittee on Health

Statement of Janet M. Marchibroda, Chief Executive Officer, eHealth Initiative

June 4, 2008

Chairman Dingell, Ranking Member Barton; Chairman Pallone and Ranking Member Deal of the Subcommittee; and Honorable Committee Members, thank you for holding this hearing related to the Discussion Draft of legislation to amend the Public Health Services Act to promote the adoption of health information technology (IT).

The eHealth Initiative (eHI) is an independent, non-profit multi-stakeholder organization whose mission is to improve the quality, safety and efficiency of health care through information and information technology. eHI engages multiple stakeholders, including clinicians, consumer and patient groups, employers, health plans, health IT suppliers, hospitals and other providers, laboratories, pharmaceutical and medical device manufacturers, pharmacies, public health, public sector agencies, and its growing coalition of more than 200 state, regional and community-based collaboratives, to reach agreement on and drive the adoption of common principles, policies and best practices for mobilizing information electronically to improve health and health care in a way that is responsible, sustainable, responsive to each stakeholder's needs—particularly patients, and which builds and maintains the public's trust.

The Need for Coordinated Action in Healthcare

The U.S. health care system is continuing to face many challenges, including increasing health care costs, the rising number of uninsured, and issues related to both quality and safety. For example, health care spending in the United States is expected to increase from 16% of the gross domestic product-or $2 trillion, to 20% of the GDP-or $4 trillion by 2016.[1] Quality is also of great concern to policymakers, health care leaders, and the general public. According to a study published by the New England Journal of Medicine, U.S. adults receive about half of recommended health care services.[2] And poor quality translates into higher costs. According to the Commonwealth Fund-sponsored U.S. Scorecard on Health System Performance, the current gap between national average rates of diabetes and blood pressure control and rates achieved by the top ten percent of health plans translates into an estimated 20,000 to 40,000 preventable deaths and $1 to $2 billion in avoidable medical costs.[3]

Chronic disease plays a significant role in both cost and quality in the United States. The number of Americans with chronic disease is increasing. More than 125 million Americans had at least one chronic care condition in 2000, while this number is expected to grow to 157 million by the year 2020.[4] As baby boomers continue to age, the number of individuals living with chronic conditions will continue to increase. While 12.7% of the population during the year 2000 was age 65 or older, this number is expected to grow to 20% by the year 2030.[5]

Concerns about America's health and health care are also shared by consumers. According to a 2006 Kaiser Family Foundation survey, over half (54%) of American adults are

dissatisfied with the quality of health care and almost a third (31%) are very dissatisfied.[6] In addition, over 81% of Americans are dissatisfied with the cost of health care in the U.S., with a majority (56%) very dissatisfied.[7] According to the Kaiser Health Tracking Poll related to the 2008 presidential election conducted in December 2007, health care ranks second behind Iraq as the top issue that the public wants the presidential candidates to talk about with 35% of respondents citing Iraq as the top issue and 30% citing health care as the top issue, in response to an open-ended question.[8]

The U.S. health care system is not well equipped to address growing issues around quality, safety and effectiveness in health care. Because of the highly fragmented nature of the system, information about the patient is stored in a variety of locations largely in paper-based forms which cannot easily be accessed. As a result, clinicians often do not have comprehensive information about the patient when and where it is needed most--at the point of care, and those responsible for managing and improving the health of populations do not have the information they need to measure performance and facilitate response and improvement. Most importantly, patients do not have access to all of the information they need to manage their own health and health care.

The introduction of health IT and health information exchange holds great promise for addressing many of the barriers to high quality, safe and more effective health care. Interoperable health IT and health information exchange--or the mobilization of clinical information electronically--facilitates access to and retrieval of clinical data, privately and securely, among different entities involved in the care delivery system, to provide safer, more timely, efficient, effective, equitable, patient-centered care.[9]

While there has been great interest in using health IT and health information exchange to address health care quality and efficiency challenges, health IT adoption rates continue to be low. Best estimates based on high quality surveys indicate that 24% of physician offices, 16% of solo practitioners, and 39% of large physician offices are using electronic health records.[10] In addition, as noted above, while there are several health information exchange initiatives across the United States, only 32 report that they are currently exchanging health information, and many are experiencing difficulties with achieving sustainability. Issues related to standards, financing and privacy are all addressed in the Discussion Draft.

These low adoption rates are due to a number of factors, including the lack of standards adoption that would enable interoperability of health IT systems across the care system; concerns about privacy and confidentiality of electronic information; and most significantly, the misalignment of incentives, resulting in the lack of a sustainable business model for health IT and health information exchange.

Building Consensus Among Multiple, Diverse Stakeholders on a Blueprint for Change

In October 2007, eHI released the eHealth Initiative Blueprint: Building Consensus for Common Action, which represents multi-stakeholder consensus on a shared vision and a set of principles, strategies and actions for improving health and healthcare through information and information technology. Through a broad, collaborative and transparent process led by eHI's multi-stakeholder leadership, development of the Blueprint involved nearly 200 organizations representing the many diverse stakeholders in health care.

One of the key themes of the eHI Blueprint, and eHI's work in general, is that we recognize that health IT is not an end unto itself, but a means to an end—which is higher quality, safer, more value-driven, and accessible health care for all Americans. The eHI Blueprint defines how health care IT can support key health care improvement strategies, including engaging consumers, transforming care delivery, and improving population health, while also aligning financial and other incentives and managing privacy, security, and confidentiality.

The Discussion Draft takes a thoughtful approach to addressing many of the current challenges associated with accelerating the adoption of health IT to improve the quality, safety and efficiency of health care. Many of the legislative provisions are designed to address key policy areas that to date have hindered the adoption and effective use of health IT, including financing for certain types of providers; supporting the sustainability of health information exchange efforts; the prioritization, planning and support of efforts that will speed the adoption of standards for interoperability; and federal leadership related to the development of policy and a framework for protecting privacy and security of health information.

I am delighted to tell you that in February of this year, the eHealth Initiative and its members recognized that to move forward in areas where Congressional leadership is needed, we must embark on an effort to gain consensus across the many stakeholders in health care on legislative provisions that will improve the ability of providers, consumers, health plans, employers and others to accelerate the effective use of health IT. We believe that a key factor inhibiting the passage of a comprehensive piece of health IT legislation to date has been the in-fighting that takes place in Congress among different sectors of the health care community. Broad consensus is sorely needed.

eHI is uniquely positioned in that we serve as not only an historically successful neutral convener, but also as an unbiased and balanced advocate for appropriate federal policy. As such, on February 14, 2008, we began a process to achieve common agreement on the specific actions that Congress can and should take to improve the quality, safety and efficiency of health care through information and information technology, in a way that is responsible, sustainable, responsive to each stakeholder's needs—particularly consumers, and which builds and maintains the public trust. Through the eHI Consensus Legislation process, we have engaged stakeholders in a spirited debate to find common ground on a path forward, building on the *eHI Blueprint: From Consensus to Common Action*, which was released in October 2007. This collaborative effort with our members has just resulted in the first complete draft of this consensus legislation, and we are now embarking on an even broader vetting process to ensure that we achieve consensus among all stakeholder groups in health care.

As part of this statement, we are sharing the results of not only how the eHI Blueprint--but also how our emerging Consensus Legislation--compares with the Discussion Draft. Overall, we are pleased to report that there are many common themes among the Discussion Draft and the Blueprint and accompanying draft Consensus Legislation.

Standards for Interoperability and the Role of Government

Mr. Chairman, your legislation would, among other things, create two committees to address policies for information sharing and standards for interoperability that reflect those policies. We agree that the federal government should play a lead role in setting a policy framework for privacy, security, and appropriate uses of electronic clinical information as we begin to develop and connect national, state and local, community-based health care networks across the country.

In this new health information environment where the decentralized flow of clinical information is needed to support care delivery, consumer engagement and improvements in population health, consumers must trust that their health information is protected and used for appropriate purposes. Without this trust, the transformation of American health care enabled by information technology will stall. The federal government, in partnership with health care stakeholders and especially consumers, should spend the next year creating a comprehensive framework for protecting privacy and security of health information.

We agree that standards adoption is needed to support the interoperable exchange of health information electronically. Our consensus legislation calls for a public-private partnership to support the identification, harmonization, testing and adoption of standards for interoperability, that are based on consensus health care priorities, and which are directly aligned with a comprehensive policy framework with development by leadership within the federal government. The federal government must play a key role in this standards-related entity if it is to succeed—both within governance and through its financial support, and federal health programs should be required to adopt the consensus standards, to speed their adoption within the private sector. The public-private partnership should be both transparent and inclusive—placing special emphasis on the involvement of consumers. Furthermore, the public-private partnership must quickly develop, publish and gain broad public input on a strategic plan or roadmap of the standards identification, harmonization, testing and adoption process, to provide certainty and facilitate planning by those who develop, purchase, and rely upon health IT systems

Financing Health IT Adoption and Effective Use

As noted in eHI's June 2007 report on value and sustainability for health information exchange, both national and local efforts focused on health IT adoption and health information exchange suffer from a reimbursement system that largely encourages both volume and fragmentation in healthcare. As a result, there are no incentives—and in fact, disincentives exist for the sharing of information by clinicians, hospitals and other providers, labs, and payers.[10]

Leadership is needed across both the public and private sectors to address the long-term and complex financial sustainability issues related to health IT interoperability which stem from America's current payment system. Enhancements to payment policy are needed that reward not only higher quality and more efficient health care, but also offer in the early years of adoption, other incentives that will support the foundational health IT underpinnings needed to achieve better outcomes.

While changes to payment policy are outside the scope of this legislation, we are pleased to see a number of grant and loan provisions in the draft legislation, along with an important

study on reimbursement incentives. Our draft consensus legislation also calls for a similar study. We also found consensus among our members regarding the general grants and loan provisions for health care providers and health information exchange initiatives.

In terms of funding for health information exchange, eHealth Initiative's research findings reveal the importance of local collaboration to facilitate health IT adoption and the mobilization of information electronically between health care organizations. Supported by a set of experts in economics, finance and health care, and utilizing lessons learned from learning laboratories in ten regionally-based health information exchange efforts, the eHealth Initiative Foundation--with funding support from the Health Resources and Services Administration (HRSA)--learned that sustainable health information exchange is indeed possible, but is hampered by the entrenched infrastructure resulting from many years of a third-party, fee-for-service reimbursement system that has resulted in a fragmented delivery system which creates little demand for, and in fact, engenders much resistance to the sharing of information across health care organizations.[11]

Given this fact, up-front funding for initiatives that demonstrate financial need is critical, and we are pleased to see that the grant application would require demonstration of a sustainable business plan, involvement from diverse stakeholders and other key elements which are critical to ensuring that federal dollars support long-term sustainability, not just short-term start-up needs. In our consensus legislation, we have also proposed a loan program for health information exchange, and we encourage you to consider this additional approach as well.

Financing for up-front adoption of health IT is also critical in overcoming the barriers posed by our fee-for-service payment system. As you know, many benefits of health IT adoption accrue to other entities than the providers who made the initial investment, which tends to decrease some of the return on investment for providers.

Loans for providers is an approach we support. It allows health care providers to have access to the capital they need, while also having personal investment in the outcome. In our consensus legislation, our members proposed an idea we would like to submit for your consideration—tying a portion of the loan to meeting quality measures specified by the Secretary, and forgiving that portion of the loan when those quality measures are met.

We believe this will help address one of the most central disagreements in the area of financing—whether to finance the tool itself (health IT), or to incentivize higher quality and more efficient care in a way that makes adoption of health IT the best course of action. There is no agreed upon approach, and it is not clear that only one approach will work. Introducing some loan forgiveness tied to meeting quality measures encompasses both schools of thought.

We are also pleased to see grants made available for providers in need, especially those in rural or medically underserved areas. These are critical segments of the market that cannot be left behind, and our consensus legislation includes a similar approach.

Another idea proposed by members in our consensus legislation process has been to create technology savings accounts that allow physicians in small practices to set aside pre-tax dollars in order to save up for health IT investments. While we are still exploring this approach with stakeholders, we believe it offers promise and encourage you to explore it as well.

Protecting Privacy and Security

Mr. Chairman, there is no doubt that protecting the privacy and security of health information is of paramount importance if this work to adopt information technology and use it effectively to improve quality, safety and efficiency is to succeed.

I would like to begin by sharing with you the vision for protecting privacy and security that was developed by our members and leadership as part of the 2007 eHealth Initiative Blueprint process:

> In a fully-enabled electronic information environment designed to engage consumers, transform care delivery and improve population health, consumers have confidence that their personal health information is private, secure and used with their consent in appropriate, beneficial ways. Technological developments are adopted in harmony with policies and business rules that foster trust and transparency. Organizations that store, transmit or use personal health information have internal policies and procedures in place that protect the integrity, security and confidentiality of personal health information. Policies and procedures are monitored for compliance, and consumers are informed of existing remedies available to them if they are adversely affected by a breach of security. Consumers trust and rely upon the secure sharing of healthcare information as a critical component of high quality, safe and efficient healthcare.

In this new information environment, we believe federal leadership is needed to identify and propose a comprehensive framework for protecting privacy and security and are pleased to see this would be required by our draft bill within one year of enactment.

We also recognize that health information exchange initiatives are playing new roles in the health care system, and our consensus legislation process reflects that, as does your draft bill. While we approached the issue in two different ways, the theme is the same—that consumers need confidence that these initiatives are governed by a protective regulatory or legal framework. While many of these initiatives today consider themselves Business Associates under HIPAA, your bill would require them to be such.

Our consensus legislation took a slightly different approach—calling for the Secretary to study and subsequently create a different category of Covered Entity under HIPAA. We recognize that the Covered Entity designation today would mean more permissibility regarding uses of data than some are comfortable with, which is why the Secretary would need to study appropriate activities and design parameters around those activities designed to support high quality, safe and effective health care. We are looking forward to exploring this approach with our members and other stakeholders moving forward.

We are strongly supportive of a national consumer education campaign regarding privacy and uses of health data, and we are pleased to see its inclusion in your draft legislation.

A Common Path Forward

Our discussions with stakeholders across the health care system at the national, state and local levels reveal that the health care system is so fragmented that collaboration across the multiple stakeholders in health care is crucial to defining and implementing solutions that are not only patient-centric, but which will also work within the system.

The eHI Blueprint offers a shared vision of a high-performing health care system, where all those engaged in the care of the patient are linked together in secure and interoperable environments, and where the decentralized flow of clinical health information directly enables the most comprehensive, patient-centered, safe, efficient, effective, timely and equitable delivery of care where and when it is needed most – at the point of care.[12]

Clearly there is need for federal leadership for moving this vision forward, particularly as it relates to providing a framework for policies related to privacy and security; and providing grant and loan funding to spur the market in the absence of true market forces.

Suggested Actions for National Leadership

There are several areas where federal leadership can make an important contribution toward transforming the quality, safety and efficiency of our nation's health care system through information and information technology.

- **Addressing Privacy and Security Policies**: The federal government should continue to lead and expand upon its efforts to develop a framework for privacy and security, leveraging the work of the current AHIC and drawing upon other work conducted by the federal government, as well as the private sector.

- **Aligning Incentives:** As noted in eHI's June 2007 report on value and sustainability for health information exchange, both national and local efforts focused on health IT adoption and health information exchange suffer from a reimbursement system that largely encourages both volume and fragmentation in healthcare. As a result, there are no incentives—and in fact, disincentives for, clinicians, hospitals and other providers, labs, and payers to share information.[13] Leadership is needed—across both the public and private sectors to address the longer-term, complex, financial sustainability issues related to health IT interoperability which stem from America's current payment system. Enhancements to payment policy are needed that reward not only higher quality, more efficient health care, but also offer in the earlier years other incentives that will support the foundational health IT underpinnings needed to get to better outcomes and federal leadership is required to move this work forward.

- **Driving Standards Adoption:** The harmonization and adoption of national standards for interoperability are critical to facilitate the information sharing needed to drive improvements in the quality, safety and efficiency of care. The federal government has made significant progress in this area, and a public-private partnership which is closely aligned with a policy committee focused on privacy and confidentiality can continue to provide leadership for this important work.

- **Addressing Disparities:** The federal government is already playing a leadership role in addressing disparities, but several opportunities exist for more leadership in the area of using health IT as a tool to close the differential gaps.

- **Providing Technical Assistance:** The eHealth Initiative Foundation's research on value and sustainability also made it clear that the next 24-36 months are a critical time on the ground, in terms of the success of health information exchange initiatives designed to mobilize clinical information electronically to support improvements in healthcare quality, safety and efficiency.[14] Widespread failures will set this effort back by many years, and the federal government has an opportunity to provide leadership and support to these important community initiatives. We are pleased that your draft legislation includes codifying the AHRQ National Resource Center, and hope that as the market accelerates with widespread adoption, mechanisms to provide support to especially small physician practices will mature. In fact, our consensus legislation calls for both the AHRQ Resource Center and a national network of organizations such as Quality Improvement Organizations, to undertake these efforts and ensure both progress and effective use of health IT.

  In addition to the work being conducted by the Office of the National Coordinator to test prototypes for a nationwide health information network, communities need tools and technical assistance to help them achieve financially sustainability. To achieve sustainability, these communities need "hands-on help" in developing and applying successful business models, which both the 2006 and 2007 eHealth Initiative Survey results tell us is their number one challenge.[15] The Department of Health and Human Services has played a federal leadership role in supporting this work, and we hope that continued efforts will help to ensure success.

Finally, the federal government cannot do this work alone. Public-private partnerships--operating both at the national and local levels--are needed to gain consensus, provide leadership and provide a common path forward that is workable, sustainable, and will result in significant improvements in the quality, safety and efficiency of care.

END NOTES

[1] Centers for Medicare and Medicaid Services, 2007.
[2] McGlynn EA, Asch SM, Adams J, et al. "The Quality of Health Care Delivered to Adults in the United States". N Engl J Med 2003;348:2635-2645.
[3] The Commonwealth Fund. *Why Not the Best? Results from a National Scorecard on U.S. Health System Performance*, New York: The Commonwealth Fund. 2006.
[4] Wu S. Green A. *Projection of Chronic Illness Prevalence and Cost Inflation. RAND Health*, Santa Monica, California: RAND Corporation; 2000.
[5] U.S. Bureau of the Census. Projections of the Total Resident Population by 5-Year Age Groups and Sex With Special Age Categories: Middle Series, 1999 to 2100. (NP-T3). Washington, D.C. January 2000.
[6] 2006 Kaiser Family Foundation "Health Care in America" Survey.
[7] Wu S. Green A. *Projection of Chronic Illness Prevalence and Cost Inflation. RAND Health*, Santa Monica, California: RAND Corporation; 2000.
[8] Kaiser Health Tracking Poll. Information provided by the Public Opinion and Media Research Program, December 20, 2007.
[9] eHealth Initiative. *eHealth Initiative Second Annual Survey of Health Information Exchange at the State, Regional and Community Levels,* http://toolkit.ehealthinitiative.org/assets/Documents/eHI2005AnnualSurveyofHealthInformationExchange2.0.pdf August 2005. Accessed June 2008.
[10] Blumenthal D, DesRoches C, Donelan K, Ferris T, Jha A, Kaushal R, Rao Sowmya, Rosenbaum S. *Health Information Technology in the United States: The Information Base for Progress.* Robert Wood Johnson Foundation, MGH Institute for Health Policy. George Washington University School for Public Health and Health Services the Health Law Information Project. Available at http://hitadoption.org/downloads/annual_report_2006.pdf
[11] eHealth Initiative. *Health Information Exchange: From Start-up to Sustainability.* Developed by the eHealth Initiative Foundation with support from the Department of Health and Human Services Health Resources and Services Administration. Washington, D.C. May 2007.
[12] Institute of Medicine. Committee for Quality in Health Care in America. *Crossing the Quality Chasm: A New Health System for the 21st Century*. Washington, DC: National Academy Press; 2001.
[13] eHealth Initiative. *Health Information Exchange: From Start-up to Sustainability.* Developed by the eHealth Initiative Foundation with support from the Department of Health and Human Services Health Resources and Services Administration. Washington, D.C. May 2007.
[14] eHealth Initiative. *Health Information Exchange: From Start-up to Sustainability.* Developed by the eHealth Initiative Foundation with support from the Department of Health and Human Services Health Resources and Services Administration. Washington, D.C. May 2007.
[15] eHealth Initiative. Improving the Quality of Healthcare through Health Information Exchange: Selected Findings from eHealth Initiative's Fourth Annual Survey of Health Information Exchange Activities at the State, Regional and Local Levels. December 2007.

June 3, 2008

The Honorable John D. Dingell
Chairman, Committee on Energy and Commerce
United States House of Representatives

The Honorable Joe Barton
Committee on Energy and Commerce
United States House of Representatives

The Honorable Frank Pallone, Jr.
Committee on Energy and Commerce
United States House of Representatives

The Honorable Nathan Deal
Committee on Energy and Commerce
United States House of Representative

Dear Chairman Dingell and Representatives Barton, Pallone, and Deal:

We are writing to applaud your proposed legislation (the "Discussion Draft") to promote health information technology adoption and establish a framework for protecting the privacy and security of Americans' personal health information. As members of the Consumer Partnership for e-Health, a non-partisan group of consumer, labor, patient, and research organizations representing over 127 million people, we believe that health information technology and exchange (HIT/HIE) are critical underpinnings of a more patient-centered health care system. They can facilitate better coordination of care, encourage higher quality and more efficient care, increase system transparency, and empower consumers to more actively engage in health care decision-making. At the same time, such a system raises serious concerns among consumers about personal privacy, data security, and the potential misuse of their information. 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.

Your proposed legislation takes very positive steps toward achieving a balance between promoting HIT/HIE and protecting personal health information. These steps are consistent with our coalition's Consumer Principles for Health Information Technology in the following ways:

- **Promoting individuals' access to their health information** by requiring covered entities that have an electronic medical record to maintain a log of all disclosures for treatment, payment, and health care operations and giving patients a right to receive an accounting of such disclosures.
- **Helping consumers have better knowledge and understanding about how their health information may be used** by requiring HHS to fund a public education initiative on the uses of protected health information (PHI) and designating an individual in each regional office of HHS to offer guidance and education to covered entities, business associates and the public on their rights and responsibilities related to PHI.
- **Granting individuals more control over whether and how their health information is shared** by tightening the definition of "marketing" under the current HIPAA Privacy Rule so that consumers have the right to consent to uses of their health information for marketing.
- **Protecting the privacy, security, and confidentiality of an individual's health information** by requiring regional or local health information exchange networks to include

plans for the privacy and security of individually identifiable health information and notification of breach in order to be eligible for federal grants; applying the HIPAA security rule and penalties to business associates; requiring notification of breach by covered entities and business associates; and requiring breach notification by vendors of personal health records. In addition, the legislation's requirement that HHS issue an annual report on compliance with the HIPAA Privacy and Security Rules will provide greater transparency of federal enforcement efforts, and further encourage entities holding PHI to strengthen their privacy and security protections.

- **Ensuring transparency and accountability for how various entities handle and use the information entrusted to them** by establishing Policy and Standards Committees that will conduct deliberations and make recommendations in a transparent and publicly accountable fashion, as required by the Federal Advisory Committee Act. The legislation also appropriately structures the authority and functions of the two committees to ensure that a sound policy framework governs the adoption of technical standards, implementation specifications, and certification criteria. We also strongly support the inclusion of consumer and health care worker representatives on the Policy and Standards Committees.

We look forward to working with you to advance this legislation, and identify the following specific topics for additional discussion:

- Ensuring that efforts to advance adoption of HIT/HIE are appropriately integrated into broader health system changes that will effectively improve the quality of patient care, decrease errors, and improve the affordability of health coverage. As recently noted by the Congressional Budget Office, adoption of HIT alone will not be sufficient to achieve the high quality, affordable health care system that all Americans deserve. Evaluation of the impact on quality, safety, and cost of full HIT and HIE integration will be vital.
- Strengthening the building blocks for health system reform by:
    - Supporting the development and endorsement of national performance measures to give health care providers, purchasers and consumers the tools they need to deliver and receive high quality care, facilitate quality improvement, and advance opportunities to make comparisons against regional and national benchmarks.
    - Providing a pathway for the release of federal health claims data to allow for the public reporting of quality performance information at the individual provider level.
- Addressing the potential benefits and risks of achieving an electronic health record for all Americans by 2014.

We are delighted to offer our strong support for this Discussion Draft. Thank you for your leadership and commitment to achieving a modern, high performing health care system that enhances patient care and engenders consumers' trust.

Sincerely,

AARP
AFL-CIO
AFSCME
American Federation of Teachers
Childbirth Connection
Consumers Union
Department for Professional Employees, AFL-CIO
Health Care for All
International Union, United Auto Workers
National Consumers League
National Partnership for Women & Families
SEIU

Members of the Consumer Partnership for eHealth

June 4, 2008

The Honorable John D. Dingell, Chairman
Committee on Energy and Commerce
United States House of Representatives
Washington, DC

The Honorable Joe Barton, Ranking Member
Committee on Energy and Commerce
United States House of Representatives
Washington, DC

The Honorable Frank Pallone, Jr., Chairman
Subcommittee on Health
Committee on Energy and Commerce
United States House of Representatives
Washington, DC

The Honorable Nathan Deal, Ranking Member
Subcommittee on Health
Committee on Energy and Commerce
United States House of Representatives
Washington, DC

Dear Committee Members:

On behalf of the Confidentiality Coalition, thank you for this opportunity to share our perspectives and concerns about discussion draft legislation to promote greater adoption of health information technology (HIT) and enact new provisions related to the privacy of health information.

The Confidentiality Coalition was founded to advance effective patient confidentiality protections and is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacy benefit managers and pharmacies, health information and research organizations, and others. For more than ten years, the Coalition has been led by the Healthcare Leadership Council, an association which brings together the chief executive officers of the nation's leading health care companies and institutions.

Since April 14, 2003, confidentiality of patients' medical records has been protected by the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. The Coalition believes that the HIPAA Rules strike the appropriate balance between protecting the sanctity of a patient's medical information privacy and ensuring that necessary information is available for providing quality health care and conducting

vital medical research, especially given the scrutiny that both rules received during the rulemaking process.

We have laid out our thoughts regarding Title III of the draft discussion below.

Notification of Breaches (Section 302). The Confidentiality Coalition believes that the confidentiality of patient medical information is of the utmost importance. We must maintain the trust of the American patient as we strive to improve health care quality. As part of that trust, patients should feel that those organizations they trust to use and disclose their information will alert them when health information is improperly disclosed and, consequently, could cause harm. As organizations move to electronic records and systems, auditing trails and other sophisticated tools are making it easier to detect when such improper disclosures occur. Entities that currently are covered under the HIPAA Privacy and Security Rules already maintain business practices and policies that result in notification when the subjects of breached information are at risk of harm as a consequence of that breach. Many of these policies are a result of various state laws and regulations based on specific requirements and risk-based standards for when a notification of breach is necessary.

The Coalition is concerned that the proposed discussion draft would not provide individuals with meaningful notice based on the risks associated with any such breach. The language as drafted does not include some of the provisions found in state law that have been helpful in determining when a breach is necessary and warranted. Rather, under the proposed draft, notification would be required for all breaches involving personal health information, regardless of whether or not it includes any personal identifiers. Rather than using risk-based standards based on the potential for economic harm, comparable to those used in the financial services sector, notification would be required for any breach that could reasonably result in substantial harm, embarrassment, inconvenience, or unfairness. The ambiguity of the requirements could lead covered entities to issue notification requirements at little, if any, benefit to the patient. By ensuring that breach notification is required only when there is a risk-based potential for harm to the patient, we can ensure that individuals take notifications seriously and act accordingly to protect themselves.

Additionally, requirements that the notice be given within 15 business days and be vetted through major media outlets in the case of insufficient contact information should be re-worked to develop a more targeted approach to notification. We look forward to working with you on refining this section of the discussion draft.

Applying Security and Privacy Penalties to Business Associates (Sections 301/311). From a principle of fairness, the Coalition supports the notion that, to the extent not already provided under HIPAA, privacy rules should apply to all individuals and organizations that create, compile, store, transmit, or use personal health information.

Under the Privacy Rule, any person or organization that performs certain functions or activities on behalf of a covered entity, or provides services to a covered entity that involve the use or disclosure of individually identifiable health information, is considered a "business associate." Business associates already are required to comply with uses and disclosures and other safeguards specified by their contract with a covered entity. This includes provisions that prohibit business associates from making any use or disclosure of protected health information that would violate the Privacy Rule. A business associate contract must also authorize a covered entity to be able to terminate the contract if the covered entity determines the business associate is in material violation.

As written, the proposed discussion draft would require business associates to comply with the administrative, physical, and technical standards for security currently required of covered entities under the Security Rule, as well as provisions under the Privacy Rule related to contractual relationships currently reserved for covered entities; Business associates who do not comply would be subjected to civil and criminal penalties. The Coalition is concerned that the draft language would subject business associates to the full requirements under the HIPAA Rules layered on top of the additional responsibilities and penalties enumerated within their contracts with covered entities. Care should be taken to ensure that organizations are not subjected to duplicitous requirements and obligations that would hinder or prevent them from offering services that are vital to the delivery of health care.

Furthermore, the covered entities category within the Privacy Rule was crafted to address patient privacy as it relates to specific activities that are undertaken by providers, health plans, and clearinghouses in order to efficiently and safely deliver services related to treatment, payment, and other essential healthcare operations. Privacy as it relates to business associate functions may be better addressed through covered entity contracts that allow for only certain limited uses and disclosures.

Requested Restrictions on Certain Disclosures of Health Information (Section 312(a))
We respectfully request that the language in this section be re-framed so that out-of-pocket payments made to providers that constitute co-payments and deductibles do not fall within the category of payments that would restrict the covered entity from disclosing personal health information to a health plan for purposes of carrying out payment. Providers are obligated to disclose health information related to plan beneficiaries when co-pays and deductibles are paid, not only for legal contractual reasons, but also so that plans and patients will know when deductibles and co-payments are met.

We also ask the committee to consider the effect of this provision on Medicare beneficiaries who are covered by Part D for their prescription drug coverage. Many beneficiaries fall into a donut hole or gap in coverage after exceeding a limited payment amount for their prescription drugs. Once the beneficiary meets this limit, he or she must pay out of pocket for his or her prescription drugs until a higher threshold is reached. This could put Medicare Part D beneficiaries in a predicament in which they would not

exit the donut hole because the plan would not be aware of the payments that patients were making out of pocket.

"Limited Data Set" (Section 312(b))
The Privacy Rule already requires that health care providers and health plans use the minimum necessary amount of personal health information to treat patients, pay for care, and conduct other essential healthcare operations. We ask for clarification regarding the requirement that covered entities first attempt to rely on the "limited data set" as defined under the HIPAA Privacy Rule before utilizing the "minimum necessary" standard for use, disclosure, or request of protected health information. For a number of reasons spelled out below, we are concerned that this provision could have a deleterious effect on patients and providers.

First, we are concerned that providers who have become accustomed to using the minimum necessary standard would have to "back into" the use of a "limited data set," a requirement that could prove particularly onerous for those parties that already maintain administrative systems and procedures based on the previous standard. Second, while we appreciate that the language allows for a covered entity to disclose the minimum necessary to accomplish the intended purpose if needed, we question whether using a limited data set as a default would serve to increase the privacy of health information. Third, we also respectfully request clarification as to whether or not the use of a limited data set would require entities to enter into new data use agreements as currently required under the Privacy Rule. Requiring covered entities to enter into such agreements would run directly counter to the balance established under HIPAA that allows for the acceptable uses and disclosures of individually-identifiable health information within health care delivery and payment systems.

We look forward to working with you to better understand the intent behind this provision. We do not want patients to experience delays in payment or elsewhere as a result of this provision.

Accounting of EMR Disclosures (Section 312(c)). As mentioned, the Coalition supports, to the extent possible, the use of auditing trails and other electronic tools to track disclosures of personal health information and engender further patient trust in HIT. As drafted, the proposed legislation would require providers that utilize electronic medical records to provide an individual, upon request, an accounting of disclosures made within the past six years, including those made for the purposes of carrying out treatment, payment, or health care operations. While many entities that hold protected health information today have certain capabilities that allow them to track many types of uses and disclosures, the use of an electronic medical record, as defined in the draft, does not necessarily imply the capability to track and account for every disclosure related to treatment, payment, and health care operations. Furthermore, it may be, at present, impossible to implement such a system in a timely fashion. Even entities operating

sophisticated electronic medical record systems today would require substantial storage capacity to conduct such accounting. This would be incredibly taxing on their systems.

It should also be noted that during development of the HIPAA Rules, the Department of Health and Human Services (HHS) considered and accepted comments addressing the possibility of removing the current account exception for disclosures regarding treatment, payment, and health care operations. They ultimately rejected that approach on the basis that it would be unduly burdensome on covered entities and result in accountings of little added-value to the individual requesting such information.[1]

Conditioning Health Care Operations (Section 313). The Coalition respectfully requests clarification as to the intent of this section. We are pleased that the language aims to preserve the existing exceptions to the definition of marketing under the HIPAA Privacy Rule as these exceptions have been extremely important in allowing covered entities to make communications aimed at furnishing treatment and conducting essential health care operations. We caution further scrutiny of this section to ensure that it does not require covered entities and their business associates to obtain authorization before making communications that patients find helpful and valuable to their care.

Study on Vendor Privacy and Security Requirements (Section 314). As stated, the Coalition believes that, to the extent not already provided under HIPAA, equitable privacy rules should apply to all individuals and organizations that create, compile, store, transmit, or use personal health information. The Coalition therefore supports the proposed report by HHS and the Federal Trade Commission (FTC) to identity privacy and security requirements that should be applied to vendors of personal health records (PHRs). However, in order to ensure that no organization that is currently subject to privacy and security requirements under HIPAA is subjected to multiple and duplicitous requirements, the proposed language should be modified to direct HHS to only focus on those PHR vendors that are not currently covered entities or business associates under HIPAA. We respectfully suggest modifying the definition of vendor [section 300(14)] so that it excludes entities that are covered entities or business associates as defined by the HIPAA regulations.

Temporary Breach Requirements for Vendors (Section 315). Additionally, the Coalition is appreciative that, in the interest of fairness, the discussion draft aims to also establish requirements for notification of breach that apply to vendors of personal health records. In addition to our previous concerns about the potential workability and patient benefit of such requirements, the Coalition questions why a separate provision was included for vendors that allows them to presume no risk, and therefore eliminates their obligation to notify in instances where individually-identifiable health information is encrypted. We respectfully ask that this encryption exception be included in the requirements for covered entities and business associates as well. As a general comment, we also

[1] 65 CFR 82739

respectfully suggest that notification of breach requirements for covered entities and business associates under HIPAA should closely mirror those established for other entities, such as vendors. By harmonizing these requirements to the extent possible, the legislation would promote fairness and consistent patient expectations as to what constitutes a meaningful and materially harmful breach of their information.

Conclusion.

All members of Confidentiality Coalition support the transition to a nationwide, interoperable system of electronic health information. Broader use of HIT has the ability to safeguard the privacy of patients and health care consumers while, at the same time, enable the confidential sharing of information that is critical to the timely and effective delivery of health care, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions.

The Coalition would like to thank the Subcommittee for the opportunity to provide our perspectives on these matters. We recognize the leading role that you have played in promoting legislation that would further improve the efficiencies and quality of the health care system.

We look forward to working with you on privacy and security provisions included in the discussion draft. We ask that you carefully review our concerns and would appreciate the opportunity for further discussion on these matters.

Sincerely,

Mary R. Grealy,
President
Healthcare Leadership Council for the Confidentiality Coalition

Testimony Before House Committee on Energy & Commerce Subcommittee on Health

Hearing on Health Information Technology and Privacy Legislation

June 4, 2008

Submitted by Michael Kirshner, DDS, MPH
Program Director, Health Informatics
Oregon Institute of Technology

Mr. Chairman and Members of the Committee, thank you for allowing the Oregon Institute of Technology to submit written testimony for today's important hearing on health information technology legislation.

Due to advancements in healthcare industry technology and the belief that the adoption of these technologies will help control costs, reduce medical errors and improve patient care, **there is an immediate need for talented, highly trained professionals in health informatics** to meet specialized workforce demands. Meeting the need nationwide will require an increase in the training and education of a skilled workforce – particularly at the baccalaureate level.

Graduates with degrees in Health Informatics will supply the capabilities required to move toward successful widespread adoption/maximization of health information technologies. These professionals will have the ability to integrate network architecture, database design, clinical systems/practices, health care finance/accounting and health care quality controls. Training these professionals now is critical. Federal legislative support in terms of funding and grant opportunities to undergraduate baccalaureate-level education is an important step in this vital process.

With the emergence of EMRs and other health care IT, there is a high and growing demand for skilled health informatics specialists. In order to adequately plan and address workforce needs, we must accurately understand its scope. According to US Bureau of Labor Statistics (BLS) data, employment of health information professionals is expected to grow by over 30 percent nationally through 2016, more than twice the growth rate for all occupations. Clearly, this is a large number. Unfortunately it does not tell the entire story of the demand for health care information technology workers.

According to a recent university study, conducted by Oregon Health & Sciences University (OHSU), at least 40,000 more health information technology professionals are needed to assist hospitals in adopting and utilizing advanced information systems as a means to improve patient care, minimize errors and control spiraling costs. That number will increase dramatically when non-hospital settings and other health care related industries are included in the study.

Health information technology includes a range of disciplines from medical records professionals, often referred to as health information managers, to health informatics professionals or health informaticians. Health information management professionals are differentiated from health informatics professionals in that the former focus on the accumulation, storage and accuracy of patient data, while the latter focus on the design, development and utilization of patient and enterprise-wide data systems.

Whereas health information management operates in the domain of medical records, billing and data regulatory compliance, health informatics is grounded in the domain of IT and systems analysis. Health informatics possesses a foundation and background in information infrastructure and architecture, computer information systems, as well as knowledge of clinical data and business operations in health care. Both health information management and health informatics are important aspects of health IT. However, with the ever-increasing digitization of health care services and the increasing number of information-based systems, the role of health informatics is becoming a critical and essential link in the chain of health care quality and cost control.

Unfortunately, the current supply of qualified health care information technology professionals is insufficient to meet the workforce shortage problem. Despite the fact that there are more than sixty graduate programs in the US in medical and health informatics, there are fewer than five fully accredited university-based baccalaureate programs in health informatics. The vast majority of workers needed to meet the shortage require undergraduate and baccalaureate-level education and training.

So, where will the new workers come from? How will they be trained and prepared to meet the needs of the marketplace? And what academic structure is most appropriate for each occupational group?

The primary source of preparation for entry level and middle management workforce is through undergraduate education, both at the Associate and Bachelor degree levels. According to the BLS, the educational requirements for health information management professionals are high school and some college, most often a 2-year AA degree, whereas, the educational requirements for health

informatics and IT-related health professions are designated as a Bachelors degree.

Local community colleges offer certificates or 2-year Associate degrees in health information management with a primary focus on preparing graduates to accurately code, maintain and manage patient medical records.

At present the only Bachelor degree program in Health Informatics in Oregon, and one of the few in the nation, is at the Oregon Institute of Technology. OIT has a long history of undergraduate academic excellence in Allied Health Professions and Computer Science and Engineering. The Health Informatics program leverages OIT's expertise in these two areas. The curriculum is specifically designed to train students and working professionals in the competencies needed for health care IT and health informatics workers. This program applies computer and information science to the delivery of heath care and prepares students for computer systems analysis, database administration and knowledge management unique to health care.

The OIT health informatics program is designed to attract students from four groups in order to meet the workforce needs. The first group is incumbent workers, those currently employed in health care or in IT. Training incumbent workers, who have domain expertise while allowing them to continue working, will provide quick entry into the workforce. The OIT program in Portland is structured to meet the needs of working adults.

The second group is current college students who have an interest in an IT or health care career path. OIT is working closely with local community colleges and universities to introduce students to career opportunities and to develop total career pathways for students in health care IT and health informatics, extending from community colleges through graduate programs, such as those at OHSU.

The third group is high school and middle school students exploring career options. Due to the low level of awareness of the academic discipline and career opportunities of health informatics or even health care IT among high school students, significant efforts need to be undertaken to inform and motivate students to seek a career in health care IT. Attracting middle and high school students is an investment in the future. OIT is actively involved in Sponsored and Pre-college programs that outreach to middle and high school students and counselors.

Finally, there is also a large group of currently employed allied health care professionals who need to be trained in heath care IT as part of their core competencies. According to the Association of Schools of Allied Health Professions, Past President David Gibson, the future of many allied health

professions will depend on the degree to which they are integrated into the health information highway. OIT is working with Allied Health Programs to develop and offer core curriculum and Continuing Professional Education courses in health care IT and informatics.

Undergraduate education is a cornerstone in meeting the workforce needs for the large number of entry level and incumbent health information management, health care IT and health informatics professionals. OIT is committed to training highly skilled professionals prepared to enter the workforce.

The problem is clear – we need to meet a health care IT workforce shortage by quickly building a qualified workforce in the US. The solutions will require legislation and federal involvement, plus universities and colleges working together in preparing the health care IT and informatics workforce for today and tomorrow. Financial opportunities are essential. Direct funding and grants available to undergraduate universities to develop and improve health informatics curricula will provide the foundation in building a workforce required to develop, implement, train users and evaluate health care IT applications. We hope you will consider this vital national need as the House Energy & Commerce Committee moves forward on health information technology legislation.

Thank you again for allowing us to submit this written testimony today.

About OIT:

Founded in 1947, Oregon Institute of Technology (OIT) is one of seven distinguished institutions belonging to the Oregon University System. OIT's applied technology education model fosters an environment of experiential, high-touch learning so students are world-ready and employment-ready when they graduate. OIT students have a 97% success rate (employment or graduate school) and the highest salaries upon graduation of any Oregon public university.

Oregon Institute of Technology earned the No. 10 spot among Baccalaureate Colleges in the West in the 2008 edition of "America's Best Colleges" by U.S. News & World Report, the nation's leading source of service journalism and news. The university also ranked fourth in the Western ranking of the Top Public Baccalaureate Colleges. OIT is one the few colleges in the country offering a Bachelor of Science degree in the highly demanded field of Information Technology with a Health Informatics Option.

Office of the Secretary

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

June 3, 2008

The Honorable John D. Dingell
Chairman
United States House of Representatives
Committee on Energy and Commerce
Washington, DC 20515-6115

Dear Chairman Dingell:

Thank you for your request for the views of the Federal Trade Commission ("FTC" or "Commission") regarding the Committee's draft legislation addressing privacy, data security, and breach notification issues related to health information technology. We applaud the goals of the provisions of the draft legislation that relate to the FTC and look forward to working with the Committee as it refines its proposal.

The draft legislation encourages the promotion of health information technology and quality by codifying the establishment and activities of the Office of the National Coordinator within the Department of Health and Human Services ("HHS"). It further seeks to strengthen the Health Information Portability and Accountability Act ("HIPAA") privacy and security requirements, extending certain of these requirements to "business associates" of covered entities. Importantly, the draft recognizes the development of a variety of new technologies supporting online medical records – technologies designed both to enhance communication among medical providers and provide consumers with greater access to their medical records. Many of these new technological developments did not exist and were not contemplated when HIPAA was enacted. In particular, the Committee's draft addresses vendors of "personal health records" or "PHRs," a type of electronic health record that is created and controlled by the consumer. A number of these vendors currently are not covered under HIPAA.

The Committee draft includes several requirements that relate to the Commission. In particular, it requires HHS to consult with the Commission in the development of recommendations to Congress regarding privacy, data security, and breach notification standards for vendors of "PHRs." The recommendations, due within one year, also must address which of these agencies is best equipped to enforce such requirements. In the interim, the draft requires PHR vendors to follow temporary breach notification requirements, enforceable by the Commission with civil penalties available for violations, that are similar to those that the bill would impose on HIPAA-covered entities. Notice would be required when a vendor discovers that personally identifiable health information has been acquired by an unauthorized person, but

would not be required if the vendor "reasonably determines that there is no reasonable risk of substantial harm, embarrassment, inconvenience, or unfairness." The draft also sets forth a rebuttable presumption that a breach involving encrypted data does not create a reasonable risk requiring notification, and it requires the FTC to issue guidance regarding the notification standard within one year of the legislation's enactment.

As the Committee is aware, the FTC has been at the forefront in protecting consumer privacy and promoting data security. As part of this mission, the FTC engages in vigorous law enforcement of a number of privacy and data security laws,[1] and it conducts consumer and business education campaigns to raise awareness about how to protect sensitive consumer data.[2] Since 2001, the Commission has brought twenty cases against companies that allegedly failed to provide reasonable protections for sensitive consumer information.[3] Further, recognizing that

---

[1]The principal privacy and data security laws enforced by the FTC are: the Federal Trade Commission Act, which prohibits a wide variety of entities from engaging in unfair or deceptive acts or practices; the Gramm-Leach-Bliley Act, which requires financial institutions to safeguard customer data and limits how such data can be used and shared; and the Fair Credit Reporting Act, which limits the use of consumer report data and imposes safe disposal obligations on entities that maintain such data.

[2]For example, last year the Commission released a brochure providing guidance to businesses on basic steps they can take to secure their systems. *See, e.g.*, Protecting Personal Information, A Guide for Business, *available at* http://www.ftc.gov/infosecurity. *See also* www.onguardonline.gov.

[3]*In the Matter of The TJX Companies*, FTC File No. 072-3055 (Mar.27, 2008, settlement accepted for public comment); *In the Matter of Reed Elsevier Inc. and Seisint Inc.*, FTC File No. 052-3094 (Mar. 27, 2008, settlement accepted for public comment); *United States v. ValueClick, Inc.*, No. CV08-01711 (C.D. Cal. Mar. 13, 2008); *In the Matter of Goal Financial, LLC*, FTC Docket No. C-4216 (April 15, 2008); *In the Matter of Life is Good, Inc.*, FTC Docket No. C-4218 (Apr. 18, 2008); *United States v. American United Mortgage*, No. CV07C 7064, (N.D. Ill. Dec. 18, 2007); *In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Apr. 3, 2007); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006); *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006); *United States v. ChoicePoint, Inc.*, No. 106-CV-0198 (N.D. Ga. Feb. 15, 2006); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005); *In the Matter of Nationwide Mortgage Group, Inc.*, FTC Docket No. 9319 (Apr. 12, 2005); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005); *In the Matter of Sunbelt Lending Services*, FTC Docket No. C-4129 (Jan. 3, 2005); *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002); *In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002).

there are gaps in the existing data security laws,[4] the Commission has recommended, both on its own and as part of the President's Identity Theft Task Force,[5] that Congress consider enacting new federal standards to protect sensitive consumer data. Such standards would require any company that holds such data to implement reasonable measures to protect it and, further, to provide notice to consumers in the event of a breach. The Commission also has recommended that it be granted civil penalty authority to enhance its enforcement efforts in data security cases.

Although the Commission has had extensive experience in enforcing and regulating privacy issues, its work to date on medical privacy has been limited.[6] Indeed, with many medical privacy issues addressed by HIPAA and HHS, the Commission's involvement in this area has not been as extensive as its involvement in other areas affecting consumer privacy. A number of PHRs and related products and services, however, fall within the FTC's jurisdiction. The FTC therefore recognizes that it has a role to play in addressing the privacy and data security issues raised by PHRs, and welcomes the opportunity to work with HHS on these issues. In particular, the FTC applauds the draft's directive that HHS, in consultation with the FTC, study and develop recommendations regarding the privacy, data security, and breach notification requirements applicable to PHRs. Because PHRs are new and evolving entities – with both similarities to, and differences from, HIPAA-covered entities – we believe such an examination is needed to develop appropriate protections in this area. The FTC also applauds the draft's attempt to address privacy concerns about PHRs – and particularly notification to consumers in the event of a breach – in the interim, and its grant of civil penalty authority to the Commission in connection with

---

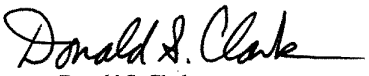
[4]In particular, there currently is no federal data security or breach notification law; rather, there are sector-specific requirements, such as those noted above.

[5]The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, at 35-37, *available at* http://www.idtheft.gov.

[6]The FTC held a public workshop on April 24, 2008 that examined innovations in health care delivery, including the use of PHRs. *See* http://www.ftc.gov/bc/healthcare/hcd/index.shtm. *Cf. In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002) (alleging that company misrepresented the security provided for medical information collected from consumers).

enforcement. We look forward to examining the bill in greater detail and addressing particular provisions, such as the trigger for notification,[7] and we welcome the opportunity to work with Congress and HHS on this issue.

By direction of the Commission.



Donald S. Clark
Secretary

cc: Joe Barton, Ranking Member
Frank Pallone, Chairman, Subcommittee on Health
Nathan Deal, Ranking Member, Subcommittee on Health

---

[7]Indeed, although there are a number of existing breach notification models and standards in the financial privacy area, the Commission has not yet examined whether this trigger is appropriate to reach the concerns raised by breaches involving medical data. For example, the Commission's proposed standard – focusing on breaches that create a significant risk of identity theft – may not be broad enough to encompass the concerns raised by breaches of medical data.