AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

LEGISLATIVE PROPOSALS TO PROMOTE ELECTRONIC HEALTH RECORDS AND A SMARTER INFORMATION SYSTEM

HEARING

BEFORE THE

SUBCOMMITTEE ON HEALTH

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

MARCH 16, 2006

Serial No. 109-114

Printed for the use of the Committee on Energy and Commerce

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE

30-339PDF WASHINGTON : 2006

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) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON ENERGY AND COMMERCE

JOE BARTON, Texas, *Chairman*

RALPH M. HALL, Texas
MICHAEL BILIRAKIS, Florida
Vice Chairman
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
Vice Chairman
VITO FOSSELLA, New York
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
C.L. "BUTCH" OTTER, Idaho
SUE MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee

JOHN D. DINGELL, Michigan
Ranking Member
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MIKE DOYLE, Pennsylvania
TOM ALLEN, Maine
JIM DAVIS, Florida
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas

BUD ALBRIGHT, *Staff Director*
DAVID CAVICKE, *General Counsel*
REID P. F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON HEALTH

NATHAN DEAL, Georgia, *Chairman*

RALPH M. HALL, Texas
MICHAEL BILIRAKIS, Florida
FRED UPTON, Michigan
PAUL E. GILLMOR, Ohio
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
STEVE BUYER, Indiana
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
SUE MYRICK, North Carolina
MICHAEL C. BURGESS, Texas
JOE BARTON, Texas
(EX OFFICIO)

SHERROD BROWN, Ohio
Ranking Member
HENRY A. WAXMAN, California
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
GENE GREEN, Texas
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
LOIS CAPPS, California
TOM ALLEN, Maine
JIM DAVIS, Florida
TAMMY BALDWIN, Wisconsin
JOHN D. DINGELL, Michigan
(EX OFFICIO)

CONTENTS

	Page
Testimony of:	
Nelson, Ivo, Healthcare Industry Leader, Global and Americas, IBM	17
Braithwaite, William, Chief Clinical Officer, eHealth Initiative and Foundation for eHealth Initiative	31
Mertz, Alan, President, American Clinical Laboratory Association	40
Vaughan, Bill, Senior Policy Analyst, Consumers Union	45
Newman, Mark, President and CEO, Evanston Northwestern Healthcare, on behalf of Healthcare Leadership Council	56
Pyles, James C., Attorney Member, Powers, Pyles, Sutter and Verville, P.C.	96
Detmer, Dr. Don E., President and Chief Executive Officer, American Medical Informatics Association	127
Additional material submitted for the record:	
Braithwaite, William, Chief Clinical Officer, eHealth Initiative and Foundation for eHealth Initiative, Response for the Record	154
Mertz, Alan, President, American Clinical Laboratory Association, Response for the Record	155
Newman, Mark, President and CEO, Evanston Northwestern Healthcare, on behalf of Healthcare Leadership Council, Response for the Record	158
Pyles, James C., Attorney Member, Powers, Pyles, Sutter and Verville, P.C., Response for the Record	161
Detmer, Dr. Don E., President and Chief Executive Officer, American Medical Informatics Association, Response for the Record	164
Blue Cross and Blue Shield Association, prepared statement of	166
Peel, Deborah C., MD, Founder, Patient Privacy Rights Foundation, prepared statement of	171
Advanced Medical Technology Association, prepared statement of	177

LEGISLATIVE PROPOSALS TO PROMOTE ELECTRONIC HEALTH RECORDS AND A SMARTER INFORMATION SYSTEM

THURSDAY, MARCH 16, 2006

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

The subcommittee met, pursuant to notice, at 10:10 a.m., in Room 2123 of the Rayburn House Office Building, Hon. Nathan Deal (chairman) presiding.

Members present: Representatives Deal, Shadegg, Burgess, Barton (ex officio), Brown, Waxman, Green, Capps, Baldwin, and Gonzalez.

Staff present: Chuck Clapton, Chief Health Counsel; Melissa Bartlett, Counsel; Ryan Long, Counsel; Nandan Kenkeremath, Counsel; Bill O'Brien, Legislative Analyst; David Rosenfeld, Counsel; Brandon Clark, Policy Coordinator; Chad Grant, Legislative Clerk; John Ford, Minority Counsel; Chris Knauer, Minority Investigator; Purvee Kempf, Minority Counsel Amy Hall, Minority Professional Staff Member; Bridgett Taylor; Minority Professional Staff Member; Jessica McNiece, Minority Research Assistant; and Jonathan Brater, Minority Staff Assistant.

MR. DEAL. I will call the hearing to order. We are pleased to have all of you with us today, and certainly another distinguished panel for this hearing. Let me tell you at the outset that this is one of those days where we have a lot of votes on the Floor. In fact, we are going to be interrupted almost at the point we begin today with a series of about 10 votes on amendments that were debated yesterday, and we'll be on the Floor for an immediate vote this morning.

We thought we would try to get started and call the committee hearing to order and maybe get in a few opening statements before we have to leave. We will try to accommodate your time constraints because you are our guests and we appreciate your presence with us today. We also have a great deal of interest in the subject matter of this hearing and in the testimony that is going to be presented. We will have several members of the full committee who are not members of our Health Subcommittee who will probably be joining us, and I invite them

to join us on the dais. I would ask unanimous consent for them to be allowed to submit their written statements for the record, and without objection that is so ordered.

There may come a time in the questioning stage where, depending on how long we have been going in this hearing and the availability of time, that we will address the issue of their ability to ask questions at that point in the hearing process. We would certainly at this point ask unanimous consent for those members of the full committee to be allowed to submit written questions for the record in the event time does not allow their oral questions, and without objection that is so ordered.

I will now recognize myself for an opening statement. As I said, we are pleased to have such a distinguished panel of guests with us today, and I look forward to your testimony on a subject that I think is certainly at the very top of most people's concerns when we talk about healthcare reform. The use of better information technology and healthcare holds the potential not only to save lives but also money. In the creation of an electronic system to track medical records hopefully we will reduce medical errors and help eliminate inefficiencies and waste in the current system.

These systems hold a potential to significantly improve healthcare 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 may seek treatment. As many of you are aware, several bills have already been introduced in Congress to deal with this general subject matter of new technologies. These proposals reflect a broad range of ideas about what can be done to create the proper incentives to encourage more healthcare providers to acquire and use healthcare information technology.

This hearing is hopefully going to be the first in a series of hearings to explain these proposals and explore what actions Congress needs to take in this area. However, we need to be cautious of dramatic legislative proposals which largely seek to regulate this budding technology area. Innovators, investors, healthcare providers, healthcare payment systems and patients will drive these changes. As a guiding principle, Congress should do nothing that would impede or limit reforms which are already transforming the market place. The President and the Health and Human Services Secretary Michael Leavitt, have both shown broad leadership in promoting this great discussion and demonstration and initial activities that hopefully will be helpful to our future.

We are also seeing many hospitals, physicians, pharmacies, and payers moving forward in the implementation of this technology. We

neither want to interfere with this effort nor overstate the government's role in innovations, applications, or basic investment decisions. Ultimately investments and the products, training, and activities to promote the use of structured information will happen piece by piece and not by a grand government design. We must also continue to provide patients with the assurance that their personal medical records will remain private and not be subject to inappropriate disclosures.

Such protections must also balance the need to be realistic and workable so that patients can reap the benefits of better healthcare through the use of IT. The adoption of new technologies holds the potential to improve accountability and empower patients with greater access to their own medical records. At the same time, safeguards must be provided to prevent hackers and other unauthorized persons from gaining access to confidential medical records. As we move forward, let us look at the many legislative proposals to promote electronic health records of health information technology in a cautious fashion. Hopefully, we in Congress can be helpful and not unintentionally slow down or misdirect the growth in the many new innovations and applications to come.

Again, I welcome our witnesses and thank you for your participation. And in the absence of Mr. Brown, I am going to recognize Mr. Waxman for an opening statement.

[The prepared statement of Hon. Nathan Deal follows:]

PREPARED STATEMENT OF THE HON. NATHAN DEAL, CHAIRMAN, SUBCOMMITTEE ON HEALTH

- The Committee will come to order, and the Chair recognizes himself for an opening statement.
- I am proud to say that we have a distinguished and expert panel of witnesses appearing before us today that will help us explore how to best increase the proper utilization of information systems in our healthcare delivery system.
- The use of better information technology in healthcare holds the potential to save lives as well as money. 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.
- These systems hold the potential to significantly improve healthcare 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.
- Several bills have been introduced with the intent of helping speed the adoption of these new technologies.
- These proposals reflect a broad range of ideas about what can be done to create the proper incentives to encourage more healthcare providers to acquire and use health information technology.
- This hearing is hopefully going to be the first in a series of hearings to examine these proposals and explore what actions Congress needs to take in this area.

- However, we need to be cautious of dramatic legislative proposals which largely seek to regulate this budding technology area.
- Innovators, investors, healthcare providers, healthcare payment systems, and patients will drive these changes.
- As a guiding principle, Congress should do nothing that would impede or limit reforms which are already transforming this marketplace.
- The President and the Health and Human Services Secretary Michael Leavitt have both shown broad leadership in promoting the many discussions, demonstrations, and initial activities that will be helpful for our future.
- We are also seeing many hospitals, physicians, pharmacies, and payers moving forward in the implementation of this technology.
- We neither want to interfere with this effort nor overstate the government's role in innovations, applications, or basic investment decisions.
- Ultimately, investments in the products, training and activities to promote the use of structured information will happen piece by piece and not by a grand government design.
- We must also continue to provide patients with the assurance that their personal medical records will remain private and not be subject to inappropriate disclosures.
- Such protections must also balance the need to be realistic and workable so that patients can reap the benefits of better healthcare through the use of IT.
- The adoption of new technologies holds the potential to improve accountability and empower patients with greater access to their own medical records.
- At the same time safeguards must be provided to prevent hackers and other unauthorized persons from gaining access to confidential medical records.
- As we move forward, let's look at the many legislative proposals to promote electronic health records of health information technology cautiously.
- Hopefully, we in Congress can be helpful and not unintentionally slow down or misdirect the growth in the many new innovations and applications to come.
- Again, I welcome our witnesses and thank them for their participation.
- I now recognize my friend from Ohio, Mr. Brown, for five minutes for his opening statement.

MR. WAXMAN. Thank you, Mr. Chairman. I appreciate you holding this hearing. It is an important issue. As we look forward to electronic health records and promoting smarter information systems, I want to raise the same caution that you just did. Computerized medical records pose a threat to one of the most basic privacy rights that an individual can have. Basic medical and genetic information should not be shared without meaningful informed consent, but even with consent protections against release of information, the right to be informed of any breach of privacy, the right to have access to one's own information and strong protections against the discriminatory use of the information are all critical.

Further, the maintenance of State laws that protect privacy should be a bedrock principle. We cannot take such comfort in our Federal rules that we can afford to eliminate any additional protections. And, finally, I cannot help but comment on the irony that we would even contemplate limiting State protections when we have so clearly failed at the Federal

level to adopt legislation that assures basic protections against discrimination on the basis of genetic information. This committee has jurisdiction in this area and it should exercise it. It is an important one to keep in mind. As we look at the positive side of it, we should also recognize that there is a potential negative side to this new computerized health world. Thank you, and I yield back the balance of my time.

MR. DEAL. Mr. Shadegg, you are recognized for an opening statement.

MR. SHADEGG. Thank you, Mr. Chairman, and I want to compliment you on the legislation you put in this area. I would echo the remarks you made in your opening statement. I will not make my own opening statement other than to say that while there are important gains that can be made in this area, my personal belief is we ought to also be looking at giving consumers more choice. Choice works in so many other places, and in the healthcare field we have given consumers virtually no choice. Their healthcare plan is selected by their employer in the vast majority of cases. It is handed to them from their doctor. They are told who their doctor is in any given area, and I believe we have taken them too much out of the equation. And it is critical while the gains we can make here are very important and need to be pursued, and I compliment the bill you have, we also need to be looking at advancing choice and healthcare to the greatest degree possible. With that, I yield back.

MR. DEAL. I thank the gentleman. Ms. Capps, you are recognized for an opening statement.

MS. CAPPS. Thank you, Mr. Chairman, and I want to thank you also. I am pleased that we are holding hearings on health information technology because I believe that facilitating better sharing of information between members of the healthcare community is a very important aspect of improving patient safety and quality of care. I am very excited to hear from our witnesses today, and I thank each of you for coming. I am excited by the prospect of eliminating unnecessary procedures and duplication of examinations or lab work that is often caused because of the inadequate filing and information transfer.

I am optimistic about how utilizing health information technology has the possibility of removing many of the administrative burdens that healthcare professionals, especially nurses, must devote their time to. Thinking of the people who are carrying the burden of delivery of care within our institutions and settings and the time that is so often taken away from the patient to fill out the duplicative records, and each time that is done it makes the possibility of error creep in. As we all know, the current nursing shortage crisis is only continuing to worsen. Less time spend filling out paperwork, as I said, or combing through extensive

medical histories means that nurses and other patient care providers can spend more time with their patients. That is going to mean better healthcare for patients.

I am also interested in how health information technology has the potential to reduce costly, often fatal, medical errors such as adverse drug reactions, interactions. The prospects for expanding the use of current information technology extend far beyond how we treat current patients also. Finally, I am hopeful about how digitalizing records may help serve the medical research community as long as the privacy protections are maintained, and that is a big as long as. But I think the possibility exists for doing this, and I want us to explore the ways that technology can help us with the privacy protections, as well as accessing medical research which is imperative for future developments in healthcare.

As we work to reap the potential benefits of health IT, we will face challenges in developing a method that is cost effective and accessible to all providers. Furthermore, while evaluating the different paths toward increasing the usage and improving the interoperability of health IT, we must remain concerned, as I said, about protecting patient privacy. As always, expanding the use of information technology systems lends itself to greater access of information in both positive and negative ways. We must ensure safeguards are in place which protects information from being accessed by the wrong parties or being used to discriminate against individuals. So I look forward to hearing from our witnesses today on how we can create a system that is beneficial to everyone involved in the provision of healthcare, keeping our bottom line to improve treatment and protect patient privacy. I yield back the balance of my time.

MR. DEAL. I thank the gentlelady, and am pleased to recognize my friend, Mr. Brown, the Ranking Member of the Health Subcommittee.

MR. BROWN. Thank you, Mr. Chairman. I apologize for being late and, thank the witnesses, all of you, for joining us today. We have all heard according to the Institute of Medicine report to err is human. Studies have found that deaths from medical errors range from estimates of 44,000 a year to as high as 98,000. Among the reasons cited in the report for such extremely high numbers of errors are issues like illegible writing in medical records, and the lack of coordination and communication across providers. I am pleased the committee has called this hearing today because increased use of electronic medical records is a very promising means by which to address these errors, cut down on the number of unnecessary deaths in this country, as well as improve the quality of healthcare.

Electronic medical records provide the ability to coordinate care across different healthcare sites. This means your general practitioner

can keep track of what treatments you are receiving from different specialists, helping to oversee your care, and make sure you get the services that you need. They can reduce healthcare administrative costs as duplicate folders of paper records are consolidated into one electronic record accessible from any computer in the office. Hospitals and doctor offices can establish support systems for their doctors to help them make the best decisions for their patients. Right at the bedside doctors can check for patient allergies and whether they have a family history of stroke, for example.

According to the IOM, health information technology is a key step to improving the quality of healthcare. Finally, the electronic medical records means that records can travel with patients backed up in case of emergencies. Katrina highlighted this point clearly in the wake of the hurricane. Thousands of displaced individuals with serious medical conditions found themselves with no access to their medical records. Paper records in doctor offices were unreachable or in many cases were destroyed. Patients had no record of what medications they had been taking, what dosage, what treatments they were receiving, whether these treatments had been effective or not. Breaks in care can be deadly for individuals with conditions like some forms of cancer or HIV/AIDS that require ongoing and regular treatment.

In a system of paper records stored on shelves in doctors' offices, displaced residents find themselves having to try and re-create years of medical records. In circumstances like these, electronic medical records can actually protect patients' health by allowing doctors to immediately identify healthcare needs and provide treatment in a timely manner. I do want to be clear, however, that while there are many benefits to increased implementation of health information technology we have to be very cautious about how we move forward. Over time these systems may result in savings for providers and for patients. Their development and implementation is a costly process, one that can be a heavy burden for family physicians and their practices.

We should never mandate the implementation of costly technology without adequate support, particularly for small physician practices that may not have the necessary capital. Finally, there must be adequate protections for patient privacy. We have all read the stories about stolen bank records in the last few months. Imagine the cases of stolen medical records. My own State of Ohio has enacted a series of laws expressly aimed at protecting a patient's confidentiality, a patient's ability to determine with whom and how medical information is shared in a right of action in cases of inappropriate disclosure. In particular, the State has enacted laws protecting information concerning birth defects, HIV/AIDS, and genetic tests. These are important protections. The last

thing we want to do is see an individual avoiding necessary and important medical care for fear of lack of confidentiality.

We need to put resources in to developing standards and guidance to assist physicians and medical institutions through the process of developing electronic medical record systems. However, we have to be keenly aware of finding an appropriate balance between utilizing technology and protecting patients. I look forward to hearing from all of our witnesses about how to address these issues. Thank you, Mr. Chairman.

MR. DEAL. I thank the gentleman. I recognize Dr. Burgess from Texas, a member of our subcommittee, for an opening statement.

MR. BURGESS. Thank you, Mr. Chairman. I appreciate you calling this hearing today. I do have an opening statement I will submit for the record, but I would just like to make a few observations. A few years ago in a graduate level course that I took so that I would be better able to understand the business work as I practiced medicine, I learned a startling fact that the insurance industry spent between 7 and 12 percent of their budget on information technology. The average small office such as mine spent an average of 1 to 3 percent. Clearly, we could not keep up at that rate.

We had an opportunity in this country with the Y2K, most people do not remember that now, but it was a big deal in the health industry for a time, and I used that opportunity to upgrade the computer services in my office over the objection of my partners because it did not return any real value. And it is going to be a process of educating physicians, particularly physicians my age, who did not grow up in the computer world to recognize what that value is. But that brings me to another point, and it is not really related to this discussion this morning but it is important in that we are faced with the prospect of continually cutting Medicare reimbursement for physicians year over year under the SGR formula.

And, Mr. Chairman, we have to seriously deal with that because we are going to drive out the best and brightest physicians, and I am referring to physicians my age, the 40 to 50-year-old doctor who is going to be driven away from the Medicare system. If we are going to spend all of this money, all of this investment, in information technology, you want to keep your best and brightest involved in the field. So people have said we cannot tackle it this year. It is just too big a bite, but I submit that there is no better time than the present to do that. The Ranking Member brought up health privacy issues with HIV and birth defects. As we move into the genomic it is going to become even more critical, and we have to be able to assure people, the public, that their

medical information will be private and not readily dispersible across half of the civilized world.

And then finally, Mr. Chairman, I just have this observation. In the 21st Century it almost makes no sense that we still fight things the way we do here in Congress, and while I appreciate you having this hearing here this morning, to me it just underscores that there is no committee on health in the United States Congress. The jurisdiction is divvied up between several committees, and I think it is time for the Committee on Energy and Commerce to assert its rightful place and take all of that jurisdiction so we can deal with these problems without having to go through stove pipes. With that, I will yield back.

MR. DEAL. I thank the gentleman. Another member from Texas, Mr. Green, is recognized for an opening statement.

MR. GREEN. Thank you, Mr. Chairman, for holding a hearing on electronic health records and legislation introduced by our colleagues to facilitate further development of health information. I would like my full statement to be placed in the record, and I will just talk about two incidents recently. When we had Hurricane Katrina and Rita, Katrina in Louisiana and obviously Rita in southeast Texas and southwest Louisiana, there were a couple of events that could show how important electronic records were. As both hurricanes approached the area and everyone fled, including a lot of our healthcare providers who closed their facilities, at the time they had to figure out how they were going to store their records. The benefit of electronic records is incalculable for providers who had them in place.

In Beaumont, Texas, a 19-doctor practice knew that Rita was coming and backed up their computer data with a server in a Dallas hotel room. And a week after Rita hit the practice reopened and all their data, including their patients' electronic records were there, and it reappeared as if nothing happened. The hurricanes also highlighted the need for interoperability within the EHRs. In my hometown of Houston where we received 150,000 residents from New Orleans, it was so chaotic to try to have people come in and get them rediagnosed if they did not have their medication. You did not know what dosage. But the VA stood out. If we received a veteran from Louisiana the VA medical professionals at Houston's VA medical hospital were able to access the records for these evacuees who had typically received care at the VA hospital in Louisiana.

Mr. Chairman, that shows in the real world, particularly in an emergency situation disaster, how this can be done. And I think we need to do it. I know it is costly, but the further we move it along the better it will be, not only for I think the physicians who practice for the sanctity

of their records along with our privacy concerns, but also for the delivery of medicine to our constituents. Thank you.

MR. DEAL. I thank the gentleman. Ms. Baldwin, you are recognized for an opening statement.

MS. BALDWIN. Thank you, Mr. Chairman. I am happy that we are taking this time to focus on healthcare IT. Like other Members who have spoken already this morning, I want to add my voice of support for implementation of healthcare IT. It is the healthcare topic that policy makers love to love these days. And it is easy to understand why healthcare IT is so popular. The potential for improving patient care, making better use of scarce resources, and collecting data for research is huge. Imagine the opportunities for medical collaboration that healthcare IT could provide for a rural doctor who needs to consult with a specialist who is hundreds, perhaps even thousands, of miles away or imagine the immensely powerful research data that could be de-identified and then analyzed to track the spread of Avian flu or widespread negative side effects of a popular drug. So I am encouraged that we are taking up this important topic and I hope that we will be able to have some constructive discussions on issues involving advancing healthcare IT.

But I also think we need to be very up front and clear about the issues involved and the potential pitfalls. From a provider standpoint there are many barriers to the adoption of healthcare IT. These barriers may be financial, technical, cultural, or legal, and these are all worthy of serious consideration discussing only the inter-operability or the interconnectivity issue could take us hours to fully understand it, perhaps years to reach agreement on. From the patient perspective, while patients tend to have enormous potential gains from increased access to and frankly ownership of their own health records, there are also potential pitfalls, specifically surrounding how to craft a healthcare IT system that insures patient privacy protections are not sacrificed in the name of increased efficiency.

Lastly, I think we need to be very cognizant of avoiding the situation where we have healthcare IT haves and have nots. Healthcare IT systems are expensive, and those who spend the money to put healthcare IT systems into place are not always the same people who benefit from these systems. So we need to keep moving forward keeping this in mind and looking for ways to bring responsible privacy protecting healthcare IT systems to all Americans. Thank you, Mr. Chairman, for holding this hearing.

[Additional statement submitted for the record follow:]

PREPARED STATEMENT OF THE HON JOE BARTON, CHAIRMAN, COMMITTEE ON ENERGY AND COMMERCE

Thank you, Chairman Deal, for holding this important hearing. Medical records haven't changed much since doctors and paper found each other. I suppose the filing cabinet was regarded as a giant advance in technology. But masses of fragile paper stuffed into large pieces of furniture are an anachronism here at the dawn of the information age.

We're here today to discuss the next great advance. Electronic health records will mean more than convenience for doctors' assistants. They will mean faster, better, less expensive care, with fewer of the medical errors that harm patients instead of help them.
I want to applaud President Bush and Secretary Leavitt for their leadership on this issue. I also want to recognize the many activities at HHS and in the private sector that will help speed the adoption of health information technology. Several Members have legislative proposals to help promote electronic health records and promote smarter information systems. We will review these ideas and see if there are areas where the Federal government can be helpful.

This isn't about the government deciding what's best for you, and then forcing it down the private sector's throat. The private sector will also play an important role in the development of smarter information systems. Any investment of time, resources, or money needs to provide a return on investment in health care quality and costs. When the utility is there, the investments will follow. It is very likely some elements of electronic health records will be in more standard use in the near future. I am optimistic, for example, about greater near-term adoption of e-prescribing and electronic reporting of laboratory results. Other elements may take longer.

As we review our current regulatory programs, we need to make sure that regulations promote improved coordination of care. This may mean looking at things like government payment policies and Stark and Anti-kickback provisions. The government may be able to assist the private sector in encouraging the harmonization of interoperability standards. No one should, however, see this as an easy task.

I look forward to hearing from today's witnesses and to try to identify legislative provisions that are clearly helpful, mindful of the appropriately limited role of the Federal government in choosing among innovations in technology.

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

Mr. Chairman, thank you for holding this hearing on Health Information Technology. Electronic medical records, electronic prescribing, decision support services, and the ability for systems to exchange information make it easier for physicians to do their job and patients to have more coordinated care. But this technology creates new challenges for keeping an individual's information private and protected from disclosure. And is it necessary to compromise other patient protections in order to encourage the use of health information technology?

First, over the past week, one of the biggest security breaches occurred when pin numbers for many top banks in the world were compromised. Yet loss of money does not compare to the irreparable damage that can result from sensitive health information, such as mental illness records, HIV/AIDs status, or genetic medical histories, being compromised.

In order to successfully implement electronic health records, patient concerns need to be addressed at every level. Patients are worried about the privacy and security of their health information, whether they have the right to decide to keep sensitive information out of the network, having access to their own records, and having control

over how the information is used. Providers and health plans say they want to expand health information technology to get better quality care and to coordinate care for patients. But without including patients in the process of developing a national health information infrastructure and addressing their needs, we will not succeed in having a system that patients feel comfortable taking part in and using.

Second, do patient protections need to be sacrificed? Representative Nancy Johnson and Subcommittee Chairman Deal have introduced a health information technology bill that creates an exemption from Federal fraud and abuse laws. This broad exemption would allow hospitals and health plans to give away free health information technology and services to physicians. Could this lead to biased decision-making by physicians about where to send patients who need hospital care? Do we really need to weaken the laws that protect vulnerable patients against abusive activities at a time when they need health care?

Finally, I note that a serious commitment to health information technology means putting funding behind our proposals, making available grants, loan programs, or incentive payments through Medicare and Medicaid. Without funding, we are merely providing lip service to this very important effort.

I look forward to the testimony the witnesses will present today. Thank you.

PREPARED STATEMENT OF THE HON. TOM ALLEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MAINE

Mr. Chairman, thank you for calling this hearing today to examine the current state of health information technology. Advances in HIT has shown great promise in improving the quality of health care, lowering costs, and reducing medical errors.

Maine has been at the forefront of adopting HIT. It is one of the first states to implement a statewide electronic health record-sharing system.

In January 2006, the board of directors of the "Maine Health Information Network Technology System" formalized a not-for-profit organization to implement an "Interoperable Health Information Network," which is slated to be in place by 2010. This electronic medical records system will bring critical medical data to physicians and other health care providers across the state and provide immediate and universal access to key medical information.

Having a state-wide electronic medical records system in place will ensure better, safer and more cost-effective care.

As we focus our attention on efforts to bolster the adoption of HIT nationwide and consider specific legislative proposals, I urge my colleagues to first "do no harm." We need to ensure that current patient privacy standards are not eroded. Consumers need to know that the confidentiality and security of their medical records will be guaranteed.

PREPARED STATEMENT OF THE HON. TIM MURPHY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF PENNSYLVANIA

Thank you Mr. Chairman.

As a psychologist, I have experienced a great deal of success in bringing people together. However, perhaps my greatest achievement was hosting a press conference when Senator Hillary Rodham Clinton (D-NY) and former Speaker Newt Gingrich (R-GA) stood side by side to save tens of thousand of lives and hundred of billions of dollars. In May of last year, Senator Clinton and former Speaker Gingrich attended a kick-off ceremony to discuss my introduction of the first health information technology (Health IT) legislation of its kind aimed at dramatically transforming the way health care is delivered in this country. The 21st Century Health Information Act (H.R. 2234)

promotes the move towards secure, confidential electronic health records and interoperable regional health information networks.

I was pleased to work with my colleagues including Energy and Commerce Health Subcommittee Chairman Deal (R-GA), Ways and Means Health Subcommittee Chair Nancy Johnson (R-CT) and U.S. Department of Health and Human Service Secretary Michael Leavitt on legislative proposals to ensure that our 18th century paper file system catches up with our 21st century medical care. Many of the provisions from my legislation including a Stark exemption to allow hospitals to buy this lifesaving technology for their doctors was incorporated into H.R. 4157, the Health Information Technology Promotion Act and I am proud to cosponsor this legislation before the Subcommittee today.

Health IT is not computers, wires, hardware, software, and PDAs, it is fewer errors, less infections and mistakes, lower cost, better quality and a higher standard of care. It's as simple as that.

Today, voluminous paper medical records are frequently scattered between multiple hospitals and doctors' offices resulting in the likelihood that important records could be lost or not retrieved when doctors need to be making informed decisions. One study found that one in seven medical records was missing vital patient information. The paper-based, often incomplete, medical record-keeping system used by most health care providers leads to redundant tests, medical errors, and misdiagnoses. All told, the RAND Corporation reported these critical errors add $162 billion in health care costs per year. Electronic medical records (EMRs) and electronic prescribing can reduce costly medical and medication errors, while quickly and securely being able to provide a patient's medical records and tests at a moments notice.

It is my hope that this hearing will focus on continued concerns over protecting patient privacy, interoperable standards to avoid a 'Tower of Babel' where health systems can not speak to each other and leveraging technology to improve the efficiency, quality and safety of the health care system. Every day that we delay implementation is costing lives and money.

Thank you, Mr. Chairman for allowing me to participate in today's hearing, I look forward to working with you to transform health care for the 21st Century.

PREPARED STATEMENT OF THE HON. FRED UPTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. Chairman, I am encouraged that we are taking this big step forward today to examine and evaluate what needs to be done legislatively to foster the rapid development and dissemination of health information technology, including electronic medical records, and to do this in a way that will not impede further technological advances. We've got some tough nuts to crack. Protecting patient privacy, modifying anti-kickback laws to allow the development of HIT networks, and modernizing our coding systems are just three areas that come to mind immediately.

As an original cosponsor of H.R. 4157, the Health Information Technology Promotion Act, that you and Mrs., Johnson introduced, I think the bill gives us a solid starting point for progress toward a 21st Century health care delivery system—a system of efficient, coordinated, cost-effective and high-quality care. While we are second to none in the world when it comes to medical innovation, we have a system that is fragmented, vulnerable, inefficient, and fraught with preventable medical errors. We've got some catching up to do, to say the least.

Perhaps nothing offers a more compelling example of the pressing need for the widespread use of electronic medical records and health information technology than the aftermath of Hurricane Katrina. Hundreds of thousands of residents were displaced from their homes, many fleeing with only the clothes on their backs, and living in shelters and

temporary housing across the country. Neither the evacuees nor their new health care providers had access to their paper medical records, many of which were destroyed. At least 40 percent of evacuees were taking prescription medications before the storm, and many more needed medications after it. Because our nation's pharmacies have been in the forefront of electronic medical records and health information technology, five days into the disaster, a website, KatrinaHealth.org, was in the works, and shortly, doctors and pharmacists across the country could go online and find out what medications many of the evacuees they were seeing were taking and how that might affect any new medications they were thinking of prescribing.

Meanwhile, back in the Gulf, hospital roofs were dotted with what sodden paper records may have survived, weighted down with stones, and drying out in the sun.

MR. DEAL. I thank the gentlelady. And, Mr. Gonzalez, a member of the full committee, we welcome him to the dais as well. Thank you for being here. It is my pleasure now to introduce our distinguished panel, and we are just about to be interrupted with these votes but I will try to get your introductions in before that time. First of all, Mr. Ivo Nelson, Healthcare Industry Leader with IBM; Dr. William Braithwaite, who is the Chief Clinical Officer of eHealth Initiative and Foundation for eHealth Initiative; Mr. Alan Mertz, the President of American Clinical Laboratory Association; Mr. Bill Vaughan, Senior Policy Analyst at Consumers Union; Mr. Mark Neaman, President and CEO, Evanston Northwestern Healthcare; Mr. James C. Pyles, Attorney and member of a firm here in Washington, D.C.; and Dr. Don Detmer, President and Chief Executive Officer of American Medical Informatics Association in Maryland.

Gentlemen, we are pleased to have you here, and how about that for timing. We will let the buzzer ring for its required period of time here, and we have five more buzzers to go and they will start in just a second. But, Mr. Nelson, we will at least try to get your opening statement in. Let us wait for these bells to ring again. Mr. Nelson, you may proceed.

STATEMENTS OF IVO NELSON, HEALTHCARE INDUSTRY LEADER, GLOBAL AND AMERICAS, IBM; WILLIAM BRAITHWAITE, M.D., Ph.D., CHIEF CLINICAL OFFICER, eHEALTH INITIATIVE AND FOUNDATION FOR eHEALTH INITIATIVE; ALAN MERTZ, PRESIDENT, AMERICAN CLINICAL LABORATORY ASSOCIATION; BILL VAUGHAN, SENIOR POLICY ANALYST, CONSUMERS UNION; MARK NEAMAN, PRESIDENT AND CEO, EVANSTON NORTHWESTERN HEALTHCARE; JAMES C. PYLES, ATTORNEY MEMBER, POWERS, PYLES, SUTTER AND VERVILLE, P.C.; AND DON E. DETMER, PRESIDENT AND CHIEF EXECUTIVE OFFICER, AMERICAN MEDICAL INFORMATICS ASSOCIATION

MR. NELSON. Thank you, Chairman Deal, and members of the subcommittee. My name is Ivo Nelson. I am actually here from Texas so I feel quite at home with the people that are here today. I do lead the IBM Healthcare Business Consulting Services Group. IBM appreciates this opportunity to testify in support of legislative proposals to promote electronic health records in a smarter health information system. Today, there is growing consensus that a more intelligent, innovative healthcare system is within reach through better use of information technology. The IBM Corporation is fully committed to helping a smarter health system emerge as a model of 21st Century American innovation.

One of IBM's core values is creating innovation that matters to the company and to the world. Today, almost everyone agrees that dramatically improving healthcare is the innovation that matters. To that end, we are collaborating with other large employers, agencies, providers, and standards bodies to transform healthcare. Today, it is a fragmented paper-based problem. Soon it will become a highly connected system for fluid exchange of digital health information and innovative new services. As a company, we are striving to do for healthcare what the ATM system, which we helped to invent, did to launch the global infrastructure for electronic financial transactions or what the Internet browser did to catapult the Web from an academic network into the platform for innovation it is today.

With respect to pending legislation proposals, IBM supports provisions that serve three objectives: drive adoption of open standards by the Federal government in private industry; commit initial seed funding and make early policy choices; and create incentives in Medicaid and Medicare to reward quality of care. These three areas are keys, we believe, to a smarter system of health. This new model of care will unlock the value of health information and help healthcare become properly organized around its core constituents, patients.

Let me expand briefly on the three topics I have outlined. Standards interoperability are the front and center in a project called the Nationwide Health Information Network or NHIN. IBM is one of four companies developing prototype architectures through a contract awarded in 2005 by the Office of the National Coordinator of Health IT at the Department of Health and Human Services. The NHIN project can be thought of as a foundation for a medical Internet and digital infrastructure for healthcare. It was also structured with the ingenious requirement the four contractors must make their respective efforts interoperate with each other via open standards.

The success of the Internet itself is overwhelmingly due to open standards and protocol such as HTML, XML, IP, and many others. Some healthcare standards have had long use within care settings and

new standards are emerging. What is needed today is to expand the use of these standards across multiple care settings and across all of government healthcare. Federal adoption of an open standard for these core elements of medical is critical. For example, Federal agencies mandate reporting of extensive amounts of clinical information, yet do not allow information to be submitted via standardized electronic formats. I have actually attached the FDA drug adverse event reporting requirement, MEDRA, for you to take a look at.

While this example is drawn from the FDA, each of the agencies has comparable examples of reporting that does not utilize health information technology built on standards. Turning to the government's role as an early funder and policy maker, history demonstrates that a new innovation often proceeds slowly at first before a catalystic inflection point causes it to accelerate. The Internet remained an obscure academic network for decades before browsers drove its explosive growth. With nearly half of healthcare spending in the U.S. originating with the government, the public sector can have a decisive role in sparking a smarter health system for all Americans. Committing initial seed funding in making early policy choices will set the stage for growth of health information exchange. The funding for Dr. Brailer's office, the national coordinator, and projects like NHIN and PHRS are good examples of catalyzing funding. Efforts to resolve privacy issues are another.

IBM hopes to play a complimentary leadership role as an innovation partner for the business of healthcare and as a large employer providing healthcare to more than half a million IBMers and their families. Finally, establishing electronic health records for millions of citizens will require a range of incentives to accelerate adoption especially among physicians and providers. The benefits of a smarter health system will enable a historic shift in medicine when designed to reward outcomes and improve quality of care rather than today's fee for service model. Health IT is needed for this shift in reimbursement because it can ease the burden of measuring and reporting performance.

Creating powerful incentives is necessary if we are to transform healthcare, and this committee can start by implementing pay-for-performance model in Medicaid. To summarize the three points I leave you with are the Federal government can advance a smarter health system by widely deploying standards. You can accelerate the transformation of healthcare through bold seed funding and active leadership in policy areas such as privacy. Strong incentives are needed to drive adoption of electronic health records and rewarding the quality of care in medicine, and Medicaid is one of the most powerful tools available.

Mr. Chairman and members of the subcommittee, thank you for the opportunity to testify today, and I look forward to answering any questions you may have. I spend most of my time in the field with hospitals and payers so I have got a very pragmatic view, I think, of the industry we are all operating in. Thank you.

[The prepared statement of Ivo Nelson follows:]

PREPARED STATEMENT OF IVO NELSON, HEALTHCARE INDUSTRY LEADER, GLOBAL AND AMERICAS, IBM

Chairman Deal and members of the Health Subcommittee of Energy and Commerce. My name is Ivo Nelson and and I lead IBM's Healthcare Business Consulting Services. IBM appreciates the opportunity to testify in support of legislative proposals to promote electronic health records (EHRs) in a smarter health information system.

Today, there is growing consensus that a more intelligent, innovative healthcare system is within reach. Through better use of information technology, experts agree that healthcare quality can be improved and costs restrained, while protecting the privacy of patients and the security of their health data.

The IBM Corporation is fully committed to helping a smarter health information system emerge as a model of 21st century American innovation. We are focusing our software, services and expertise and combination of business and technology experience to support the transformation of healthcare from its fragmented, paper-based current state into a coherent, interconnected system. The objective is to enable the fast and fluid exchange of digital health information, applications and services that will revolutionize all facets of healthcare.

Healthcare is closely aligned with one of the three core values around which IBM organizes and manages our global enterprise: creating "innovation that matters, to the company and the world."

Today, almost everyone agrees that dramatically improving healthcare is the innovation that matters. To that end, IBM is collaborating with other large employers, agencies, providers and standards bodies on a host of efforts to spur the transition to digital healthcare. As a company we are trying to do for healthcare what the ATM system (which IBM helped invent) did to launch a global infrastructure for electronic financial transactions, or what the Internet browser did to catapult the World Wide Web from an academic network into the platform for innovation that it functions as today.

IBM supports legislative provisions that:

- Drive adoption of open standards by the federal government and private industry;
- Commit initial seed funding and make early policy choices that will set the stage for growth of health information exchange; and
- Create incentives in Medicaid and Medicare to reward quality of care, including those that can be measured and rationalized through the use of health information technology (Health IT).

These three areas — open standards, seed funding and policy commitment that catalyze change, and new incentives to reward the quality of healthcare — are the keys we believe, the keys that will open up a smarter information system for healthcare. Not only will this new model of care unlock the value of health information in a networked world, it will help healthcare evolve into a system properly organized around its core constituents—patients—and begin to make costs and quality more transparent to all.

In 2004, the President launched an initiative to make electronic health records (EHRs) available to most Americans within the next 10 years. In 2005, the Senate passed legislative reforms to Medicare reimbursement and Health IT legislation that drives toward these goals. We encourage similar action by your committee and the House in 2006.

Today, I would like to talk about the steps that this committee could take to improve healthcare, first through better use of open technology standards. Where possible, I will use examples of our own conduct and efforts at IBM.

I. Driving Standards Adoption

Achieving the vision of a nationwide health information exchange first requires interoperability: the ability for disparate health information systems to be able to talk to each other and share data in a safe and secure manner. Interoperability and standards are often mistakenly lumped together. Standards are much narrower and specify technical details. Interoperability, on the other hand, is a much broader concept that involves both atechnical and business context.

The success of the Internet itself is overwhelmingly due to the implementation of open standards, protocols, languages and architectures such as HTML, XML, HTTP, PDF and many others. In fact, almost all digital dataflow today depends on an open standard for packets of digital information called IP, or Internet Protocol.

Open standards have been profoundly embraced by most technology companies, as well as governments and the public sector around the world for many years, and for many reasons. Chief among them is that open standards work to ensure compatibility and interoperability that benefits all participants. Broadly speaking, standards have long proven their value in business and society in everything from measurements of weight and size to transformative technologies such as wireless networks.

"Open" standards are those that are freely available to all, and are created by an open decision-making process. In our world of networked information, they speed innovation, integration and collaboration in countless dimensions, including supply chain management, consumer electronics and many forms of communications.

Why is better use of standards so important? In short, better use will facilitate the easier exchange of health information, thereby helping lower costs (e.g. transaction costs), provide better information to physicians and caregivers at the point of care and improve patient safety and clinical quality.

Until we have unambiguous, clinically-relevant coding of chief complaints, prescriptions, laboratory and imaging orders and results, we hobble our ability to learn from this vast corpus of information. Outcomes analysis, long-term effects, and the identification and encouragement of best practices and quality-of-care are all dependent on capturing this information at the source. Open standards are nothing less than the means to advance the industry towards richer, more evidence-based medicine and a smarter health system.

In many cases, the standards have had long use within care settings and are simply being pressed into use for broader networks that extend across multiple care settings. Standards are used in all phases of patient care and cover everything from messaging and content, to measurement and communication. In some cases, these protocols have already achieved wide adoption, such as the **D**igital **I**maging and **Co**mmunications in **M**edicine (DICOM) format. More recently, the National Council for Prescription Drug Programs, Inc. (NCPDP) telecommunication standard was named the official format for pharmacy claims under the Health Insurance Portability and Accountability Act (HIPAA).

IBM's Standards Efforts in Healthcare

IBM has worked with providers, hardware and software vendors to develop and adopt standardized ways of describing health data, transmitting it to other computers, and

requesting processing related to that data from other computers. As specific needs for collaboration across networks become clear, new standards are developed and adopted. For example, one of the earlier standards, DICOM, was developed so that x-rays and other medical images could be shared.

IBM is a member of many key healthcare standards bodies including HL7, and was a founding member of the Eclipse Organization a leading open source community. Most recently, IBM made its entire patent portfolio available, royalty-free, to standards bodies working on open, interoperable infrastructure for healthcare and education.

Integrating the Healthcare Enterprise IBM's work on building a nationwide infrastructure for clinical information exchange (the NHIN prototype) has lead it to join an initiative called Integrating the Healthcare Enterprise (IHE). Under the leadership of HIMSS and the Radiological Society of North America, IHE is an architectural framework for exchanging information across the enterprise that can incorporate established standards to allow different healthcare enterprises to use their own choice of hardware and software. In fact, our NHIN prototype is based on IHE's work, as well as the open-standards based Interoperable Healthcare Information Infrastructure (IHII) architecture developed by IBM Research.

What is Still Missing: Federal Transition to Broad Standard's Adoption

Federal adoption of open standards for healthcare diagnoses, treatments and other core elements of medicine is critical to tip the use of these innovation drivers from desirable to necessary. When the government has adopted standards, such as the use of International Classification of Diseases and Related Health Problems (ICD-9) system for billing purposes, its market power provides a sufficient voice to finalize consensus within healthcare. The government was a principle driver for the adoption of ICD-9, CPT/HCPCS, and DRG reporting.

Existing Government Efforts Set the Stage for Adoption of Healthcare Standards
The federal government has lead numerous efforts to highlight key standards although adoption has lagged.

Consolidated Health Informatics - In 2004, as part of the Consolidated Health Informatics initiative (CHI), the HHS, DoD, and DVA agreed to endorse 20 sets of standards that enable information to be shared across agencies and serve as a model for the private sector.

Medical Language - The Department of Health & Human Services (HHS) signed an agreement in 2003 to license a standardized medical vocabulary developed by the College of American (SNOMED)

Electronic Medical Records - At the request of HHS, the international standards-setting organization known as **Health Level 7** has established a tentative standard that defines the set of functions needed in an electronic medical record.

E-Prescribing Standards - The Medicare Prescription Drug Improvement and Modernization Act (MMA) requires the Centers for Medicare and Medicaid Services (CMS) to develop standards for electronic prescribing.

Standards Harmonization Contract – HHS/ONCHIT –The Office of the National Coordinator for Health IT/HHS awarded a contract in October of 2005 to the American National Standards Institute (ANSI) to develop, prototype, and evaluate a harmonization process for health IT standards.

However, beyond the initiatives cited here, the broader federal government has been somewhat slow to adopt and drive electronic healthcare standards, and often requests that health information be exchanged using phone, mail, or manual means that don't advance open electronic standards and data exchange. As a result, healthcare care costs are higher and quality is lower than they would be if the federal government was more proactive about implementing electronic standards.

For example, federal agencies mandate reporting of extensive amounts of clinical information, yet don't require information to be submitted via standardized electronic formats. I have attached FDA drug adverse event reporting requirement – MEDRA – and an illustration from the FDA website depicting their reporting process. http://www.fda.gov/medwatch/ While this example is drawn from the FDA, each of the agencies has comparable examples of reporting that does not utilize health information technology built on standards.

Agencies need the resources, guidance and clear leadership to move away from these manual reporting systems in favor of standards-based electronic reporting. The Senate legislation includes provision to move the federal government towards standards adoption by establishing an additional requirement for standards in procurement, and requiring the option of standards based reporting to federal agencies. The provision would build on the standards identified several years ago by Secretary Thompson, while allowing further standards to be adopted as they are identified. It also allows the provider the choice of either continuing to report manually or in electronic standards.

II. The Role of Initial Funding and Policy Leadership in Sparking Healthcare Transformation

A smarter health system is clearly desirable – however, history demonstrates that innovation often proceeds slowly at first, before accelerating after a catalytic inflection point. The Internet, for example remained an obscure academic network for several decades before the Mosaic Web browser drove its explosive growth in the 1990s. The DVD player became the most rapidly adopted new technology only after manufacturers resolved two competing technology standards.

The government's role as an early funder and policy driver is vital during the initial phase of a major innovation such as the one dawning around digitally networked healthcare. Initial funding is the seed that allows healthcare system participants to develop prototypes that translate concepts into implementations. The government also plays a key role as a consensus builder on policy issues, to the benefit of both citizens and businesses. As lessons are learned from prototypes and policy development, new business models emerge over time that can carry innovation forward.

Meanwhile the nature of innovation itself is becoming more collaborative—between commercial enterprises as well as between the public and private sectors—government has a highly constructive role to play in sparking work that will unleash the ability of businesses to drive growth and productivity. A smarter healthcare system is just such entrepreneurial fire ready to be lit.

Finally, with nearly half of all healthcare spending in the U.S. originating with the federal government, the public sector can have a decisively influential role in helping engender a smarter health system for all Americans. IBM hopes to play a similar leadership role, both as large employer seeking to innovate how it delivers healthcare to its workforce, and as a business and innovation partner for many parts of the healthcare ecosystem.

Nationwide Health Information Network Architectural Prototypes.

Funding included in President Bush's Health Information Technology Plan is an important source of prototype funding. The President has requested $116 million for his health information initiative in FY 2007. While this represents a small portion of the

$5.5 billion that will be spent on health related information technology, it provides key seed money for prototypes and early learning.

The importance of standards and interoperability are front and center in a several projects pertaining to development of a Nationwide Health Information Network (NHIN). As you may know, IBM is one of four companies awarded a contract to develop NHIN architectural prototypes through a contract with the Department of Health and Human Services, Office of the National Coordinator for Health Information Technology. The four architecture prototype contractors are not building the Network, per se, but each vendor is building a prototype architecture.

The goal of the Nationwide Health Information Network (NHIN) prototype is to demonstrate major concepts that build towards the ultimate goal of a smarter, more connected information infrastructure for healthcare, including the abilities:

- To enable secure electronic exchange of healthcare information between and within healthcare marketplaces that allows for the gathering of necessary public health data while preserving patient privacy.
- To demonstrate how various healthcare marketplaces can be part of this communications network in a manner that is cost-effective and not disruptive to their current models of doing business.

These contracts complete the foundation for an interoperable, standards-based network for the secure exchange of health care information. HHS previously has awarded contracts to create processes to harmonize health information standards, develop criteria to certify and evaluate health IT products, and develop solutions to address variations in business policies and state laws that affect privacy and security practices that may pose challenges to the secure communication of health information.

IBM is following several key principles in developing a prototype architecture for the developing nationwide network. These principles are the result of IBM's experience in healthcare and other sectors. They also arise from IBM's work with many broad-based organizations in this area such as the Healthcare Information & Management Systems Society (HIMSS), the eHealth Initiative, and other information technology vendors, and privacy and technical organizations with whom we collaborate with on a daily basis.

The NHIN project promises to bring about a smarter health system by leveraging the expertise and market interests of the private sector. But it was also structured with an ingenious requirement: the four participating contractors, IBM included, must make their respective efforts interoperate across competing healthcare marketplaces via open standards. If the NHIN project can be thought of as the foundation of a "medical Internet" or digital infrastructure for healthcare, then the importance that the evolving nation-wide integrated system will be based on open standards is quite obvious.

IBM is working on the NHIN with partners in three regional communities:

Fishkill, NY
Taconic Health Information Network & Community (THINC) RHIO
RHIO/Community Leader: Dr. John Blair
2,300 physicians supporting 700,000 patients
Shared data using Healthvision

Research Triangle, NC
North Carolina Healthcare Information and Communications Alliance (NCHICA)
RHIO/Community Leader: Holt Anderson
Competitive, high-tech urban environment

Rockingham County, NC
Also members of NCHICA
Rural environment with NC and VA patients
Small, competitive practices and hospitals

In developing this prototype architecture for the evolving nationwide network, IBM is following several key principles that are the result of our experience in healthcare and other sectors. They also arise from IBM's work with many organizations in this area such as the Healthcare Information & Management Systems Society (HIMSS), the eHealth Initiative, and other information technology vendors, as well as privacy and technical organizations with whom we collaborate on a daily basis.

The NHIN project promises to bring about a smarter health system by leveraging the expertise and market interests of the private sector. But it was also structured with an ingenious requirement: the four participating contractors, IBM included, must make their respective efforts interoperate across competing healthcare marketplaces via open standards. If the NHIN project can be thought of as the foundation of a "Medical Internet" or digital infrastructure for healthcare, then the importance that the evolving nation-wide integrated system will be based on open standards is quite obvious.

Through the NHIN, it is envisioned that healthcare consumers would be empowered to access their personal health records (PHRs) using the same network that allows them to share their medical records with healthcare providers that they see in other communities. IBM's architectural prototype for the NHIN system would not be a single repository of everyone's medical records, but rather an index that points to information stored at the originating provider site. IBM believes that independent healthcare consumers, providers, and communities (as well as regional health information organizations) will set the rules for who can see what information and for what information they need.

Healthcare systems or RHIOs wish to retain control over their enterprise-wide data and will also set the business rules for how data will be exchanged. The NHIN will be a practical, community-centric approach to exchanging healthcare information in a secure, standardized way between healthcare communities in the United States.

At the conclusion of the NHIN prototype project, HHS will have four architectural prototypes to choose from or to incorporate into the adopted NHIN architecture and a dozen communities will have developed practical experience with information sharing.

IBM's prototype architecture, along with the other vendors, is part of a broader effort sponsored by the ONC including related efforts to advance the national health IT agenda. IBM continues to participate in and monitor the other ONC-sponsored efforts by The American Health Information Community, the Healthcare Information Technology Standards Panel (HITSP), Certification Commission for Health Information Technology (CCHIT), and Health Information Security and Privacy Collaboration (HISPC).

The ONC awarded contracts and named inter-related groups may supersede some of the functions and activities related in other aspects of this testimony as they evolve during the coming months. Through a series of contracts, public meetings and coordination activities, these named groups are collectively addressing standards harmonization, compliance certification, processes to develop solutions that address variations in business policies and state laws that affect privacy and security practices.

Personal Health Records

IBM can offer several examples to the Committee of our own funding and policy initiatives that may provide some guidance for similar efforts involving Medicaid. In 2005 IBM announced that it would provide personal health records (PHRs) to its entire U. S. workforce. To protect employees' privacy, the personal health record (PHR) system available to IBMers today is managed by an outside vendor and we have instituted contractual provisions and process controls in order to prevent inappropriate access to employee-specific data.

To establish their personal health record (PHR), our U.S.-based employees begin by entering basic information: medicines, allergies, major conditions, and details on their

doctors and insurance coverage. Later this year, employees' personal health records (PHRs) will grow to automatically include medical and prescription drug claims history.

Even this basic information has real utility today. It can be emailed or faxed to a provider—and even sent from a Web-enabled mobile device—or simply stored or printed out for easy access in an emergency or when traveling. The ultimate goal is to enable all types of electronic health information, including one's lab results, prescription histories, medical images and more to flow into the record to form a comprehensive portrait of a patient. Equipping and empowering patients with personal health records (PHRs) is only the start. Enabling such data to flow electronically to doctors, hospitals and other providers authorized by the patient will allow healthcare to become a highly interoperable and innovative - something it is far from today.

Early this week, CMS also issued an RFP on personal health records (PHRs) for Medicare beneficiaries. Yesterday, IBM testified to the Federal Workforce Committee about legislation to extend interoperable Personal Health Records (PHRs) to all federal employees. This Committee has the same ability to leverage existing claims data in state Medicaid programs. IBM urges you to examine the role that our federal government can play in catalyzing interoperable personal health records (PHRs) by providing them to Medicaid beneficiaries.

Just as the value of a network rises exponentially with the number of devices connected to it—the so-called network effect—the power of the personal health record (PHR) will rise dramatically the faster we can build a critical mass. What's more, with a large enough base of personal health records (PHRs), the private and public sectors will create strong incentives for physicians, hospitals, and other health system participants to begin to adopt the infrastructure for healthcare that will improve quality and reduce costs.

Interoperable personal health records (PHRs) will also drive two vital changes in the nature of healthcare itself. First, they will increasingly make the patient the center-point around which healthcare organizes itself. And second, interoperable personal health records (PHRs) and their related systems will support greater transparency across healthcare, and in many dimensions, including price and quality.

At IBM, the personal health records (PHRs) that we are providing to all of our employees in the U.S. are a prime example of this patient-centered approach. When an IBMer first goes to the Web site for their personal health record, they are offered a financial incentive to complete an employee health risk appraisal, develop a personal preventive care action plan and identify quality hospitals in their area. The process surveys a range of issues including exercise level, family histories and cholesterol control, if applicable. Based on the results, an IBMer can subscribe to receive expert information, articles and advice on how to reducing their risks. It identifies eligibility for additional benefits and services such as disease management and refers employees to those resources. Decision support tools for drug comparison and interactions, hospital quality and Leapfrog results (from the Leapfrog Group's performance measurement system) provide individual support for optimizing benefits quality and costs.

For IBM, the risk assessment tools and the personal health records (PHRs) we provide our workforce are an investment that we recoup through improvements in employee health and the significant cost savings that result. For individual employees, the incentives we provide—to take the assessment, or track their self-paced exercise regimens —are essential to helping us capture these business benefits.

Consumer Centric Healthcare

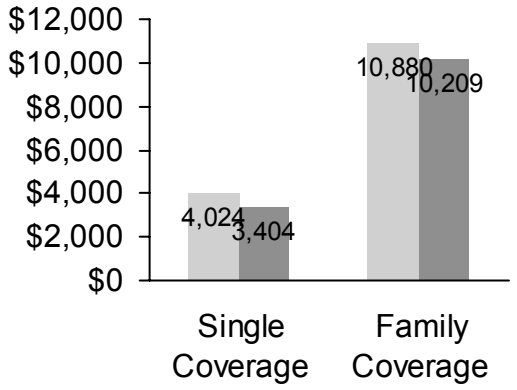
To put IBM's experience with personal health records (PHRs) in some context, I would first like to describe our broader efforts on improving employee health and reducing costs. That backdrop is, in fact, how we progressed to offer personal health records (PHRs) for our employees.

IBM provides health and health benefits of over 500,000 IBMers, retirees and dependents. In total, the IBM Corporation spends over $1.7 billion on healthcare each year. As a result of our consumer-centric health programs for our employees, IBMers are healthier and have lower health expenses than others in our industry. We have demonstrated that information-rich, patient-centric wellness programs aren't marginal benefits. They are very good business:

- IBM's employee injury and illness rates are consistently lower than industry levels.
- We have documented significant decreases in the number of health risks among IBM employees as a result of participating in our wellness initiatives.
- IBM's disease management programs have demonstrated a 9%-24% reduction in emergency room visits and a 13-37% reduction in hospital admissions resulting in an overall 16% reduction in medical and pharmacy costs adjusted for medical trend over a 2 year period.

With the health improvements, we have seen cost benefits -- IBM healthcare premiums are 6% lower for family coverage and 15% lower for single coverage than industry norms. Our employees benefit from these lower-cost as well -- they pay 26 to 60% less than industry norms. And IBM healthcare premiums have been growing significantly more slowly than U.S. health insurance premiums.

US Average Annual Premiums for Covered Workers: Industry Average vs. IBM (2005)



Critical Areas for Initial Policy Choices:

Privacy in electronic healthcare is an area of policy development with deep importance, diverse viewpoints, and great need for government leadership, both in terms of driving standards and providing catalytic early funding.

According to a 2005 survey, two-thirds of all Americans report high levels of concern about the privacy of their personal health information, with ethnic and racial minorities and the chronically ill showing the greatest concern:

- Is of a racial/ethnic minority: 73%
- Is not of a racial/ethic minority: 52%
- Has been diagnosed with a disease: 67%
- Has not been diagnosed with a disease: 63%

One in four consumers reports being aware of incidents where the privacy of personal information was compromised. In addition, they believe, erroneously, that paper records are more secure than electronic ones (66% vs. 58%). (California HealthCare Foundation)

These attitudes about privacy are reflected in the requirements consumers believe are important for electronic health information exchange. Nine of ten consumers want a system that confirms the identity of anyone accessing it. Eight of ten want to personally review who has accessed their information, and to be asked before their information is shared. (Markle) Clearly, privacy issues, and the public's perceptions of those issues, must be addressed in order for the PHR to succeed.

The HIPAA Privacy Rule has provided the bedrock for patient privacy in the U.S. and has established a baseline for privacy and security requirements for electronic health information. Many states have gone further then HIPAA to ensure patient privacy and have adopted policies that further protect patient data when stored and moved in an electronic format. These variations in policies present challenges for widespread electronic health information exchange. To assess these challenges, HHS awarded a contract devoted to privacy and security. The Health Information Security and Privacy Collaboration (HISPC), a new partnership consisting of a multi-disciplinary team of experts and the National Governor's Association (NGA), will work with approximately 40 states or territorial governments to assess and develop plans to address variations in organization-level business policies and state laws that affect privacy and security practices and pose challenges to interoperable health information exchange. Overseeing the HISPC will be RTI International, a private, nonprofit corporation who has been selected as the HHS contract recipient.

While many see privacy as a potential barrier to health information exchange, most computer systems today include a variety of privacy protections. Most people are familiar with identity-based limitations – personal IDs and passwords that must be entered in order to access a system. With little effort, privacy controls can include roles as well as identity authentication so that a billing clerk or a doctor will have the appropriate level and access to a patient's personal health information. Information technology can also provide tools to monitor who accesses data, create an audit trail for changes the data, and a watermarks to deter data theft and assert ownership of pirated copies. With paper records, there is no automated way to know, for example, if someone has accessed a record inappropriately, or even removed it or copied it.

We have the technology today to protect patients' but if privacy policies are unclear, or built on concepts such as "intent" that are difficult to translate into computer rules, technology will be of little help in formalizing privacy. Creating a smooth interface between privacy policy and technology will require a significant commitment of political will and resources. Here again, the government can play a pivotal role in stimulating and encouraging the development of privacy policies that will enable electronic healthcare to move forward faster.

III. Creating Incentives in Medicare and Medicaid to Reward Quality

Establishing a system of electronic health records (EHRs) for millions of citizens is a major societal shift, and will require a range of incentives to accelerate adoption among various constituencies. Physicians and other healthcare providers will bear the direct costs of implementing electronic health records (EHRs), as well as the indirect cost to transform their established workflow processes to take advantage of these new technologies.

The current healthcare system has well-known flaws in how treatments are reimbursed. The current model rewards the volume of services and not the quality of outcomes. This paradigm results in low quality and rising costs. Those reimbursement flaws reduce the incentive for quality improvement tools such as interoperable electronic health records (EHRs). Reforms in reimbursement methodologies and additional sources of funding will have a dramatic impact on the adoption of the electronic health records (EHRs), and the multitude of systemic benefits they reap.

The effectiveness of "carrots" for performance are why IBM supports incentives to providers to adopt electronic health records (EHRs) and other related health information technology applications (Computerized Patient Order Entry, e-prescribing, etc.).

In fact, IBM is already implementing a "pay-for-use" incentive plan to drive the use of electronic prescriptions.

In New York's Hudson Valley, where many of our employees live, we are funding a program that rewards doctors each time they use a new system for writing prescriptions electronically. Working with Dr. John Blair and Taconic Health Information Network and Community (THINC) regional health information organization, or RHIO, IBM has agreed to increase the reimbursement physicians receive if they submit prescriptions electronically. We believe that the additional reimbursement we are offering will pay for itself by reducing medication errors and increasing the use of generic drugs.

We urge this Committee to examine approaches to rewarding value through the Medicaid program. This coming year, the federal government will provide over $300 billion through the Medicaid program. It makes no sense to pay all those providers the same reimbursement rates, if the quality for some greatly exceeds — or severely lags behind — that of others. But today, Medicaid is at best neutral, and at worst negative, toward quality. Medicaid pays for the delivery of a service, not for the achievement of better health.

A number of pay-for-performance demonstration projects in Medicare are underway (see box, *right*). IBM would encourage the expansion of these pioneering efforts and application to the Medicaid program.

Medicare and Private Sector Pay-for-performance Demonstration Projects

Hospital Quality Initiative (MMA section 501(b)) - focuses on an incentives for reporting an initial set of 10 quality measures.

Premier Hospital Quality Incentive Demonstration - Under this demonstration, CMS is collecting data and provides an incentive related to performance on 34 quality measures.

Physician Group Practice Demonstration (BIPA 2000) - The demonstration rewards 10 large physicians groups for improving the quality and efficiency of health care services delivered to Medicare fee-for-service beneficiaries.

Medicare Care Management Performance Demonstration (MMA Section 649 – A three-year pay-for-performance demonstration with focused on small and medium-sized physician practices to promote the adoption and use of health information technology to improve the quality of patient care for chronically

Private Industry Efforts - Pay-for-Performance Programs and Purchasers

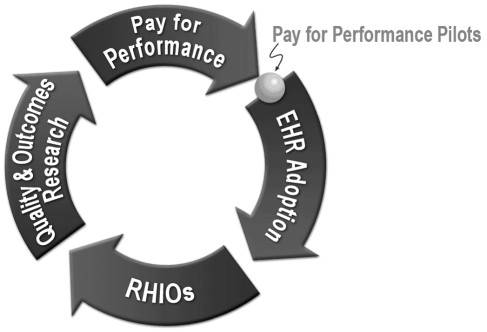
There are more then 100 pay-for-performance programs across the U.S including Integrated Healthcare Association's (IHA) pay-for-performance effort in California, The Leapfrog Group's Hospital Quality and Safety Survey and their new Hospital Rewards Program that rewards hospitals out of a savings fund, and the Bridges To Excellence program, which is an ambulatory care incentive program active in several states.

Barriers & Indicators for Success:

Electronic health records (EHRs) and a digital infrastructure to support them will enable a historic shift in medicine: rewarding outcomes and improved quality of care rather than simply paying for procedures in today's fee-for-service model. Health IT is invariably linked to this shift in reimbursement because it is needed to help document and measure performance.

Health information technology is a key to successful pay-for-performance for two reasons. First, electronic reporting can reduce the significant burden that performance reporting places on providers. Current performance measures often involve manual chart review and manual processing by skilled professionals. Electronic reporting can reduce the performance reporting burden and ease participation by providers in pay-for-performance programs.

Second, electronic reporting can align with the ongoing care process to actually improve the quality of care a patient receives, not just by documenting end results, but by alerting providers in realtime to any gaps or best practices that may have been overlooked. As a result, performance measurement carried out electronically can move from a description of quality to an operational tool that improves care. Those patients that do not receive appropriate care may be highlighted while they are interacting with providers rather than much later in reports that are submitted to reimbursers.



Naturally, the pay-for-performance model will require the support of doctors and the medical community. Financial incentives under a pay-for-performance program must be:

- Non-punitive (i.e. physicians who are unable to participate in the program should not be subject to negative updates);
- Prioritized, so that physicians are rewarded for achieving improvements for the top 20 conditions identified in the Institute of Medicine's (IOM) "Crossing the Quality Chasm" report;
- Considerate of the critical role of primary care physicians in achieving such improvements; and
- Sufficient to offset physicians' investment in health information technology and other office redesign required to measure and report quality.

We also advise that pay-for-performance programs be implemented along with reforms to change the way that physician services are valued and reimbursed, rather than grafted onto an underlying payment methodology that pays doctors for doing more, instead of doing better.

Of course, one of the most important factors in making pay-for-performance a success is the size of the incentive or bonus relative to a physician's or hospital's total revenues. While no formal studies have yet clearly documented this issue, empirical data suggest that physicians will respond to incentives only if they represent 5% or more of their total revenues.

In conclusion, creating powerful incentives in the federal health programs is necessary if we are to drive improvements in healthcare through the intelligent application of technology. Incentives for quality will undoubtedly lead toward better use of health information technology to improve healthcare. The information technology industry would like the opportunity to drive such a virtuous circle – incentives leading to better use of health IT which leads to improved quality and lower costs. This Committee can start by implementing the pay-for-performance model in Medicaid.

Summary

- The federal government can advance a smarter health system by deeply adopting and supporting open standards.
- The federal government can accelerate the transformation of healthcare through judicious seed funding of prototypes and communities and active leadership in policy areas such as privacy and security.
- Strong incentives are needed to drive adoption of electronic health records (EHRs), and one of the most powerful levers would be to reward the quality of care in Medicare and Medicaid via a "pay-for-performance" model.

MR. DEAL. Thank you, Mr. Nelson. And I again apologize but we are going to stand in recess pending these votes. There will be ten votes, so we will probably be somewhere an hour or thereabouts before we will be able to get back, but hopefully we will have a little better attendance perhaps after those first series of votes. Thank you, and we will stand in recess.

[Recess.]

MR. DEAL. We will call the hearing back to order. Thank you for being patient during the break. Dr. Braithwaite, we will hear from you at this time.

MR. BRAITHWAITE. Thank you, Mr. Chairman. Chairman Deal and distinguished members of the subcommittee, I am honored to be here today. My name is Bill Braithwaite, and I am testifying today on behalf of the eHealth Initiative and its foundation otherwise known as eHI. I serve as the chief medical officer of both organizations, which are independent, national, non-profit organizations whose missions are the same: to improve the quality, safety, and efficiency of health and healthcare through information and information technology. In addition to our main work with communities, we work actively with Congress and the Administration to support these goals and applaud their strong commitment. eHI looks forward to working with you on potential legislation in this area.

I would like to talk a little bit about the big picture. The field of healthcare today is so vast and so complex that practicing medicine with an acceptable error rate is proving to be humanly impossible without the support of integrated information technology. The number of deaths caused by medical errors in our healthcare system every year has been estimated to be around 100,000 or higher if you include all the different aspects of healthcare. I think we would all agree that this is not acceptable. In most cases the healthcare system is at fault. We still practice medicine under the old paradigm where the doctor and the patient interact from memory to arrive at recommendations of healthcare decisions for the patient.

The only way to significantly improve the quality, safety, and efficiency of our healthcare system is to bring the information system into the exam room, as it were, and to change the paradigm of clinical practice so that it routinely involves the doctor, the patient, and the computer working together to provide the best healthcare advice possible. The way to implement this new approach is through direct interaction of clinicians and patients with a Clinical Decision Support System. Such a system must be integrated into the clinical environment in a way that supports, rather than disrupts, the efficient flow of the process of healthcare. But since most of the data on which clinical decisions are made actually originate outside the exam room, the Clinical Decision Support System by itself cannot function without a way to access the sources of the clinical data, the laboratories, pharmacies, radiology centers, et cetera. This is the impetus for eHI's emphasis on interoperable health information exchange initiatives.

There are three critical prerequisites for successful implementation of health information exchange initiatives: incentives for implementation; assurances about privacy and security; and full interoperability between disparate clinical information systems. Even though all three are crucial, I will restrict this testimony to interoperability, and you will hear about the others from others on the panel.

There is still confusion in the healthcare industry about the meaning of the term interoperability. The definitions in my written testimony on page 5 come from an analysis of over 100 such definitions done by the international standards developing organization, HL7. Basically interoperability is the secure electronic communication of clinical data, like lab results from a computer in one institution in such a way that a computer in another institution can understand the precise meaning of what was said. In this case computer understanding means that the information could be processed by the receiving computer to reach conclusions about what advice to give to optimize patient care.

The terminology used to describe clinical concepts must be standardized, controlled, and coded in enough detail to differentiate between closely related conditions that might require different treatments. For example, the synonyms were originally used to identify the condition at the local hospital. At last count, for example, there were 17 different terms used in different parts of this country that all referred to the same concept of high blood pressure. Larger categories of clinical concepts typically used for reimbursement transactions are not sufficiently detailed for this purpose. Interoperability also implies that there is a standard mechanism that all participants can use to exchange the information securely. Most of us use the World Wide Web every day

and understand the power of having such a communications infrastructure available to all. Healthcare, of course, requires iron clad security as part of its infrastructure, including features not required in the standard Internet such as authentication, authorization, auditing, encryption, and digital signatures.

Successful implementation of electronic health information across institutions requires specificity, standards, and conformance testing of the results, features not currently found in most of the standards available today even after up to 20 years of development because of course the standards developing organizations have been focused on something else, the exchange of information within institutions between information systems. The sometimes heard proclamation that health information exchange should wait until the standards are done is made by those who are not fully aware of the tasks involved. Enormous progress has been made in the understanding, specification, and adoption of standards so far, but standards are not static. They must evolve to meet the continuous advances in the delivery of healthcare and can never be done. On the other hand, there are some low hanging fruit that we can address. Given that the timeline for full interoperability between clinical information systems, in my opinion, is likely to be measured in decades, what can we do in the meantime to reap some of the value of the Health Information Exchanges that we can implement today?

If we focus our resources on a few projects that can successfully reach interoperability in the short term, we can demonstrate immediate benefits for people who are working toward the same goal using consistent standards. If you ask clinicians what information is most important when they are seeing a patient without a medical record as they had to do after Katrina, they quickly list medication history, allergies, lab results, problem list, and interpretive reports. The patient, however, first wants to do without the need to fill out the same data multiple times on the medical clipboard at each provider that they go to. So let us start with those needs in mind and solve some of the immediate problems.

The industry has already made much progress on these particular needs because the demand is there, and the efforts under the contracts issued by HHS through the Office of the National Coordinator are focusing on the same situations in the context of prototypes for a nationwide health information infrastructure. Results from these funded efforts are expected by the end of this year. In addition, the important private-public sector partnerships such as the Markle Foundation's Connecting for Health initiative, with additional support from the Robert Wood Johnson Foundation, have provided a great deal of guidance on

the technical aspects and the key principles and policies for information sharing.

The standard for exchanging medication history and laboratory results is already being tested, although integration with lab test ordering is still being worked on. One approach for interpretive reports, which is one of the sort of early wins that people are looking for, is an electronic standard message that contains both a human readable representation of the data, and a structured and coded form suitable for processing by a computer. Thus, those source systems that are only capable of producing the human readable form, similar to a web page, can still participate in the electronic Health Information Exchange while those systems with more capability can include the data that is fully understood by a computer program in full interoperability. This will allow a migration over time from a simple and easy to produce form of data that is still compatible with the more sophisticated forms in both directions of communication.

MR. DEAL. Could I ask you to summarize for us, please?

MR. BRAITHWAITE. Yes. Vendors are reluctant to spend money implementing standards without customer willingness to pay for it. Providers are reluctant to pay for such features if they cannot see immediate payback. Therefore, purchasers have to be shown that the present and future value of standards-based systems and convinced to buy them whenever feasible. In conclusion, I believe we can provide appropriate incentives to implementation, adequate assurances to providers and patients about the privacy and security of their information, and support for full interoperability of our healthcare information systems. In doing so we will have set the stage for a high quality, safe, and efficient healthcare system for all Americans in their communities. eHI will be there to help you if you can do this through legislation. I would like to thank the committee for providing me the opportunity to share these insights on behalf of eHI and its foundation.

[The prepared statement of William Braithwaite follows:]

PREPARED STATEMENT OF WILLIAM BRAITHWAITE, M.D., PH.D., CHIEF CLINICAL OFFICER, EHEALTH IMITATIVE AND FOUNDATION FOR EHEALTH IMITATIVE

Summary

Health Information Exchange (HIE) initiatives are the underpinnings for a system to improve how healthcare is practiced. Recognizing that healthcare is local, the eHealth Initiative and its Foundation are supporting multi-stakeholder HIE collaboration at the state, regional and community levels through the *Connecting Communities* program. Important knowledge related to every aspect of health information exchange is resulting from this work. [see http://toolkit.ehealthinitiative.org] The current paradigm of clinical practice limits our ability to avoid errors and control costs. Only with clinical decision support systems (CDSS) integrated into the routine of clinical practice can the system support better healthcare decision making. HIE is a necessary precursor to the operation

of CDSS. Requirements for HIE implementation include incentives to stakeholders, assurances regarding privacy and security, and health information system interoperability.

Interoperability is defined with three levels of standards required, from controlled clinical vocabularies, to standardized message structures and entity identification, to a secure communications infrastructure. However, standards are not enough for interoperability. The necessity for inter-institutional exchange of data is forcing a change in the character of standards from the traditional, flexible standards currently in use between systems in the same institution to more complete, rigorous, and tested implementation specifications integrated across standards for specific use cases. Systemic barriers to the rapid deployment of this evolution must be addressed.

This process is likely to take decades before full interoperability of clinical information systems is a reality. There are some low hanging fruit that can be harvested in the near-term, however; medication history, lab results, and interpretive reports, for example. There is an existing suite of standards that addresses these areas of interoperability but most of the standards are not rigorously defined for specific use cases and are inconsistently implemented by vendors. While the HHS AHIC and ONC efforts to kick-start interoperable health information exchange is a good and positive process; it is the start of a very long road. Sustained federal leadership is crucial to achieving these goals and to promoting a smarter healthcare system over time.

Introduction

Chairman Deal, Congressman Brown, distinguished members of the Subcommittee, I am honored to be here today. My name is Bill Braithwaite and I am testifying today on behalf of the eHealth Initiative and its Foundation (eHI). I serve as the Chief Medical Officer of both organizations, which are independent, national, non-profit organizations whose missions are the same: to improve the quality, safety, and efficiency of health and healthcare through information and information technology.

In addition to our main work with communities, we work actively with Congress and the Administration to support these goals and applaud their strong commitment. eHI looks forward to working with you on potential legislation in this area.

The big picture

The field of healthcare is now so vast and complex that practicing medicine with an acceptable error rate is proving to be humanly impossible without the support of integrated information technology. The number of deaths caused by medical errors in our healthcare system every year has been estimated to be 100,000 or higher. I think we would all agree; that is totally unacceptable. And in most cases it is the system that is at fault: we still practice medicine under the old paradigm where the doctor and the patient interact from memory to arrive at healthcare decisions for the patient. The only way to significantly improve the quality, safety, and efficiency of our healthcare system is to bring the information system into the exam room, as it were, and to change the paradigm of clinical practice so that it routinely involves the doctor, the patient, and the computer working together to provide the best healthcare advice possible. The way to implement this new approach is through direct interaction with a Clinical Decision Support System (CDSS). Such a system must be integrated into the clinical environment in a way that supports rather than disrupts the efficient flow of the process of healthcare. Since most of the data on which clinical decisions are made actually originate outside the exam room, the CDSS by itself is not functional without a way to access the sources of the clinical data, the labs, pharmacies, radiology centers, etc. This, then, is the impetus for eHI's emphasis on interoperable health information exchange initiatives.

Of course, none of these technological innovations will be implemented unless there are sufficient incentives to get these systems incorporated into healthcare practice under a

sustainable business model. The needed incentives can take many forms, including pay-for-performance programs that pay providers for higher quality care delivered, and they are discussed in detail in our paper entitled, "Parallel Pathways to Quality Healthcare". In addition, none of the required information sharing will be allowed unless there are sufficient assurances to patients and providers alike that the shared information will be private and secure. In the interest of time, I will leave these two critical prerequisites for others to discuss and refer you to the eHI website for further background material [see http://www.ehealthintitiative.org/].

Interoperability

Since most data on which clinical decisions are based come from outside the exam room or other locations where clinical decisions are being made, interoperability for clinical data exchange is a basic and necessary requirement. However, in the healthcare industry there has been some confusion about the meaning of the term, 'interoperability'. The following definitions come from a meta-analysis of over 100 such definitions done by a technical committee of HL7, an international healthcare standards setting organization.

> **Interoperability** is the ability of two or more systems or components to exchange information and to use the information that has been exchanged accurately, securely, and verifiably, when and where needed.
>
> ***Healthcare* interoperability** also assures the clear and reliable communication of meaning by providing the correct context and exact meaning of the shared information as approved by designated communities of practice. This adds value by allowing the information to be accurately linked to related information, further developed and applied by computer systems and by care providers for the real-time delivery of optimal patient care.

It is important to understand all the implications of the term, 'interoperability', at different levels of abstraction from binary bits of information flowing through a wire at the bottom to the transfer of clinical knowledge at the top. At the highest levels, the context and the exact meaning of information must be preserved and made available for use. In this case, 'use' means that the information can be processed by a computer to reach conclusions about what advice to give to a clinician to optimize patient care. That means that the terminology used to describe clinical concepts must be standardized, controlled, and coded in enough detail to differentiate between closely related conditions that might require different treatments, for example. Larger categories of clinical concepts typically used for reimbursement transactions are not sufficiently detailed for this purpose. There are also a large number of clinical concepts which are referred to by different names in different geographic locations. Where locally defined terms are used in lieu of terms from a national standard controlled terminology, then mechanisms must be in place to make the translation to the national standard, a process called 'normalization', so that another location that uses its own local terms for a clinical concept can preserve the correct context and exact meaning. As simple examples that require such standardization, there are 17 different terms that represent the same concept of high blood pressure and there are 27 different potential values for the concept of sex and many different ways to encode them.

At the lowest levels, interoperability implies that there is a standard mechanism that all participants can use to exchange the information securely. Most of us use the world-wide-web every day and understand the power of having such a communications infrastructure available to all. Healthcare, of course, requires such an infrastructure to include more security features than the standard internet connectivity we all use, including authentication, authorization, auditing, encryption, and digital signatures.

In the middle levels are the standards for aggregating discrete data elements together into a meaningful message sent from one system to another in response to an event or

'trigger', standards for identifying the healthcare providers and the patients, and standards for a plethora of other elements that are unique and specific to the use case being implemented.

Clearly, interoperability requires the consistent and rigorous integration of standards of many types and necessarily from many sources. When the only electronic information exchange being considered was that between one system and the next operated by the same institution, it was easy for the technical team(s) to discuss all the specific technical decisions that have to be made before even a well defined standard can be used in a particular business use case. Once the problem is expanded to include the exchange of information among many institutions that may not even be in the same region of the country, the required degree of specificity is sorely lacking in most of the consensus standards available today and the standards development and maintenance process is perceived to be slow and cumbersome.

It is also critical, with the increasing number of participants in inter-institutional health information exchanges, that the implementations of the standards be tested be conformant to those standards. For example, HL7 standards for transmitting numeric lab results from a laboratory information system to a clinical information system or repository within an institution were some of the earliest implementations of HL7 standards. [Note that HL7 celebrated its 20th anniversary as a standards developing organization in 2006.] However, there are still implementations today where a laboratory (part of a national reference laboratory company) transmits the numeric result of a test in the comment field of a "standard" HL7 message, instead of the result field. This is accommodated in today's world by writing tailored interfaces for each data flow to bring them to a common implementation of a standard. This is expensive in the short term and untenable in the long term.

The full implementation of standards requires an effective processes for, and ongoing investment in, standards development, support and maintenance, migration, and integration. A range of supporting tools need to be developed and implemented to assist organizations in migrating to standards, including implementation guides, conformance processes, and educational materials. Demonstration and implementation projects are critical to the migration toward an interoperable, electronic healthcare system, in that they test and evaluate feasibility, uncover additional barriers and workable solutions to overcome them, provide replicable practices and tools for others, confirm value for a wide range community stakeholders, and build awareness of the benefits.

The sometimes heard proclamation that, "HIE should wait until the standards are done," is made by those woefully ignorant of the tasks involved. The many issues discussed above indicate the enormous progress that has been made in the understanding, specification, and adoption of standards. Standards are not static, however, and they must evolve to meet the continuous advances in the delivery of healthcare and can never be 'done'. To become and remain acceptable, the standards process requires some effort and participation by everyone concerned.

Low hanging fruit

Given that the timeline for full interoperability between clinical information systems is likely to be measured in decades, what can we do in the meantime to reap some of the value of the HIE that we can implement today? If you ask clinicians what the most important information is when they are seeing a patient without a medical record, they quickly iterate medication history, allergies, lab results, problem list, and interpretive reports (e.g., radiology, pathology, and operative reports that are already in electronic form through dictation). The wish list from the patient, however, starts with the data they now have to fill out multiple times on the medical clipboard. Great progress has already been made on many of these and the efforts under the contracts issued by HHS through the Office of the National Coordinator of Health Information Technology (ONC) [see

http://www.hhs.gov/healthit/] are focusing on these early wins as well as prototypes for the nationwide infrastructure. Results from these funded efforts are expected by the end of this year. In addition, important public-private sector partnerships, such as the Markle Foundation's Connecting for Health initiative [see http://www.connectingforhealth.org], with additional support from the Robert Wood Johnson Foundation, have provided a great deal of guidance on the technical aspects of health information exchange as well as key principles and policies for information sharing.

Although medication history is not directly involved in most ePrescribing initiatives, it is closely related and likely to evolve quickly based on existing standards as ePrescribing implementations proceed. Laboratory results are being exchanged in some environments today and standards for exchanging most types of results already exist. Full integration with lab test ordering is still being worked on. One approach for interpretive reports that looks promising is the use of a standard electronic message that contains both a human readable representation of the data and a structured and coded form suitable for processing by a computer. Thus, those source systems that are only capable of producing the human readable form (similar to a web page) can still participate in the HIE while those systems with more capability can include data that is fully understood by a computer program. This will allow a migration over time from a simple and easy to produce form of data that is still compatible with the more sophisticated forms in both directions.

It should be absolutely clear from this discussion and these examples, however, that we are still many years away from the fully interoperable health information exchange environment of our vision and there are several intractable barriers to more rapid progress of which we should be aware.

The business case for a vendor to incur the costs of switching to a standard is often muddled at best: short-term narrow objectives are the enemy of long-term, broad interoperability goals. Even when a vendor understands that implementing standards is good for the product, the resources to do it are not always available. Purchasers have to be informed and insist on standards-based implementations whenever feasible.

Existing standards must be 'constrained' (a term of art used by standards setting organizations) into rigorous implementation guides for each particular 'use case' (another term of art). A use case is like the outline of a play that defines the goal, the actors, the roles they play, the trigger event(s) that cause them to interact, the data elements that they must exchange, etc. Given a general use case, an implementation guide will allow an implementer to program an information system in a consistent way. It may take several implementation guides based on several standards to implement a particular use case, and the combination of these is often called an 'integration profile'.

There is a fairly well recognized first set of standards that are already being adopted for HIE. These include: HL7 data interchange standards, the HL7 Reference Information Model, the DICOM standard for imaging, the NCPDP SCRIPT prescription drug information standard, the LOINC vocabulary for laboratory tests, the IEEE/CEN/ISO 1073 medical device communication standard, the ASC X12 administrative transaction standard, HL7 Data Types, HL7 Clinical Document Architecture (CDA), and the HL7 Clinical Context Management Specification (CCOW). Work remains to be done in a number of other domains, including standards related to terminology (and their uniform distribution within the National Library of Medicine's Unified Medical Language System (UMLS)), clinical templates, clinical guidelines, representation of business rules, representation of decision support rules, data elements, disease registries, tool sets, security, identifiers, and the electronic health record.

Conclusion

In conclusion, I'd like to thank the Committee for providing me the opportunity to share my insights and expertise on behalf of eHI and its Foundation today. There is a

long road ahead but it is filled with the promise of better health for all Americans in their own communities if we work together and get it right on interoperability. Nothing could be more important and eHI will be there to help every step of the way.

APPENDIX A

Health Information Exchange: The eHealth Initiative and Foundation's State, Regional and Community-Based Program Work

Recognizing that healthcare is local—and that to stimulate change in how healthcare is delivered, one must drive change both at the national level and local levels—eHI has been focusing its efforts on supporting multi-stakeholder collaboration at the state, regional and community levels, bringing its common principles, policies and standards developed nationally to those who are delivering healthcare in markets across the U.S. This work is being conducted through the direct funding of learning laboratories at the community level and advocacy and education for additional funding to support local efforts; the building of a coalition or "community" of over 2,000 stakeholders working on health information exchange within over 250 states, regions and communities across the U.S. to share insights and effect change; and the provision of direct technical assistance to leaders within states and regions who are developing strategies and plans to facilitate HIT adoption and health information exchange.

The eHealth Initiative Foundation began its *Connecting Communities* program in FY 2003, through the leadership and foresight of Congressman C.W. Bill Young (R-FL). Though a special appropriation administered by the Department of Health and Human Services' Office of the Secretary, and in years past by the Health Resources and Services Administration's Office of the Advancement for Telehealth (HRSA/OAT), *Connecting Communities* continues to provide seed funding and technical support to a set of "learning laboratories" led by multi-stakeholder collaboratives, who are experimenting with the development of models for sustainability for their health information exchange efforts. This program will yield valuable lessons learned. Learning laboratories will inform the efforts of policy-makers, and national leaders both in the public and private sectors who must take actions to clear barriers to interoperability and health information mobility.

The 2006 *Connecting Communities* award program will provide learning laboratories for the development and implementation of sustainable business models for health information exchange and build healthcare purchaser and payer awareness of the value that health information exchange capabilities can provide in improving the quality, safety and efficiency of care to stimulate ongoing interest in supporting such activities at the state, regional and local levels. Successful awardees will have engaged the commitment of purchasers and payers representing at least 30 percent of covered lives within their markets, to participate in a pilot or implementation of an incentives program that will not only support quality goals, but also directly or indirectly, support the health information exchange capabilities which are necessary to achieve those quality goals. They will also have engaged the commitment of a large percentage of practicing clinicians--including small physician practices--who have committed to both utilizing the health information exchange capabilities, and participating in the incentives program.

The *Connecting Communities* program is also directly aiding in a task vital to our nation in the wake of Hurricane Katrina: helping to strengthen Gulf Coast healthcare services and regional electronic health information infrastructure in Alabama, Florida, Louisiana, Mississippi, and Texas by supporting public-private sector partnerships as well as assessment, planning, operational, and communications activities related to the development of health information networks within and across the Gulf States. Prior to Hurricane Katrina, work was being conducted by the Foundation for eHealth Initiative in the Gulf Coast state of Louisiana to assist in general health information technology policy efforts.

The program is also producing informative research and tools valuable to emerging health information exchanges and related policy formation. For example, the *Connecting Communities* Toolkit is a unique, multi-layered, one-stop resource offering structured, how-to synthesis of principles and tools designed to equip states, regions and local communities with the information and expertise to begin or advance local health information exchange initiatives and organizations. It offers insight into areas crucial to start-up and successful survival such as organizational structure, value creation, financing, practice transformation, quality, information-sharing policies, technical aspects and public policy and advocacy. Importantly, it is a distillation of cumulative knowledge resulting from working with multiple stakeholders in different communities. Communities contribute toolkit resources themselves in the spirit of sharing insights with their peers. Its release comes at a critical time as health information exchanges are coming into existence across America and seeking expert advice.

Through eHI's activities on health information exchange, the organization has: become the hub of best practice development and sharing for driving transformation through health information exchange, providing a full range of tools and resources for states, regions and communities who are navigating the organizational, legal, financial, clinical and technical aspects of health information exchange. It is also actively supporting stakeholders engaged in transformation and health information exchange efforts in more than 250 states, regions and communities across the U.S.

In regards to states, the eHealth Initiative has or is in the process of actively supporting 13 states across the country in developing strategies, policies, and plans for improving health and healthcare through health information technology and exchange through its State Policy Summit Initiatives. The goal of these initiatives is to help state public policy officials and key stakeholders in the healthcare and business communities develop state policy agendas and frameworks which support the rapid development and implementation of healthcare information technology and exchange. Some of the states currently being supported by eHI include Arizona, Kansas, Minnesota, New Hampshire, New York, and Ohio.

MR. DEAL. Thank you. Mr. Mertz.

MR. MERTZ. Thank you, Mr. Chairman. I am Alan Mertz, President of the American Clinical Laboratory Association. The ACLA represents the Nation's leading national, regional, and local laboratories. Mr. Chairman, most patients are probably familiar with our members, mostly by the boxes they see out in front of the doctor's office that are Quest Diagnostics or LabCorp. That is where the specimens are put in those boxes, and our members are the people who collect those specimens, transport them to a laboratory, do the testing overnight, and then report of those results usually back the next morning. Some times millions every day, and testing is absolutely a critical part of our healthcare system. It provides the physicians with the objective data they need to not only diagnose, but effectively treat and monitor disease.

Our members also have, part of the reason we are here today, an extensive history of providing these doctors and hospitals with health information technology involved in streamlining laboratory test requisition, and also speeding the delivery of test results. Let me give you just a little bit of background about laboratory testing and how important it is to the medical record, and then I will talk about some of

the legislative proposals. Laboratories and the information they provide are really the heart of the medical record. It is not well known to the layman that laboratory data actually represents 60 percent of the medical record, and while the diagnostic tests we do comprise only 1.6 percent of Medicare spending and about 5 percent of overall health spending, they influence 70 percent of clinical decision making. Not only does this information improve outcomes and decrease costs, but laboratory data is becoming an even more essential building block for assessing quality care and it is playing an increasingly critical role for quality and pay-for-performance initiatives.

The laboratories, Mr. Chairman, have made a tremendous investment in connecting to physician offices and hospitals, and it sort of served as the catalyst in the evolution of health IT. Just let me give you one example of the penetration that they have had with the physician's offices. Quest Diagnostics, our largest member, has business relationships with half of the physicians and hospitals in the United States, and this is just one laboratory company. Quest Diagnostics receives 40 percent of its orders and sends 60 percent of its results via the Internet. This is a critically important and highly valued function. It is so important that since 1995 our labs have had a limited exception under the Stark law so that they can provide these electronic connections and interfaces with physician offices.

This has been a fundamental capability for laboratories to render services to providers. It is a function that must be maintained in any changes that are made to Stark. Congressman Brown made a point at the beginning about the IOM report on errors and duplication cost and electronic ordering and results with laboratories. It is a critically important part of improving legibility, decreasing error rates, producing more timely results, and even monitoring duplicatation of testing.

Let me talk just about three quick points about H.R. 4157. We believe it has several needed improvements. Number one, we believe that if it is enacted it would further prompt adoption of health IT. We believe that any exemption in the law for Stark for IT should be carefully crafted to guard against abuses while still allowing the diffusion of IT, and we believe it strikes that balance. We also support the legislation's Federal preemption of State laws that contradict the Stark law exceptions and anti-kickback safe harbors. Today there are several State laws that are complicated and have different requirements than the Federal Stark law, and we believe that the preemption provisions there are very important.

H.R. 4157 also addresses the need for Federal preemption in State laws related to privacy. We support this provision because of the patchwork of State laws as an impediment to health information

exchange. Let me give you one example. LabCorp, another large national laboratory, has been invited to participate in regional Medicare chronic care or health support pilot programs. Chairman Deal, LabCorp has been invited to participate in an effort in your own State with CIGNA HealthCare in Georgia, as well as a program operating in central Florida operated by Green Ribbon Health. These entities will offer self-care guidance and support to chronically ill Medicare beneficiaries to help them manage diabetes and chronic heart disease problems.

LabCorp's role in the programs will be to transmit critical laboratory data to CIGNA and to Green Ribbon Health for those beneficiaries who voluntarily participate in the program. However, the State laws in Florida and Georgia governing the release of lab results have prevented LabCorp from transmitting these results. In essence, Florida and Georgia laws preclude providing test results to anyone other than the ordering physician, and there is no provision in the State laws that would allow even the patient to give their consent. These laws would effectively bar any transmittal, and even the patient's consent does not allow us to transmit those results.

Let me conclude also with the needed provisions regarding moving from ICD-9 diagnostic codes to ICD-10. Under the Medicare program the laboratories are paid by including these ICD-9 codes on their claims to provide medical necessities. These codes are provided by the physician to the laboratory, and are subsequently attached to the claim and submitted to CMS. So we really have no control of what diagnosis codes are put into the claim, and if they are not done correctly, we are not paid. So moving to the ICD-10 we want to be very careful about doing that because it is immensely more complicated. ICD-9 provides about 13,000 diagnosis codes. Moving to the ICD-10 provides 120,000 diagnosis codes, making it much more complicated.

I have attached an example to my testimony of where today there is one ICD-9 code for a sports injury, it will be replaced by something like 39 different codes, diagnosis codes included. You have to now tell whether you were struck by a baseball, golf ball, a baseball bat, and so forth, whereas you used to be able to just say this person was injured in the head by a ball. So it is much more complicated. What we are asking for here not to go ahead with this, but to give us a five-year transition period instead of two years, because of the complexity of this, and we have to train doctors as to how to do this, otherwise, we will not be paid.

So in conclusion the ACLA supports the Health Information Technology Promotion Act's new anti-kickback safe harbors and Stark law exception, the bill's proposed preemption of State privacy laws like the example that I gave, and the replacement of the ICD-9 code but with a five-year transition period. Thank you, Mr. Chairman.

[The prepared statement of Alan Mertz follows:]

PREPARED STATEMENT OF ALAN MERTZ, PRESIDENT, AMERICAN CLINICAL LABORATORY ASSOCIATION

Chairman Deal, Ranking Member Brown, and distinguished subcommittee members, thank you for the opportunity to testify today on behalf of the American Clinical Laboratory Association (ACLA) representing national, regional, and local laboratories. My name is Alan Mertz, President of ACLA, and I appreciate your interest in legislative proposals that will accelerate the widespread adoption of the electronic health record. ACLA members have an extensive history of providing the nation's hospitals and physicians with leading-edge health information technology (IT) streamlining laboratory test requisition and speeding the delivery of test results.

The Health Information Technology Promotion Act of 2005 (HR 4157) proposes several needed improvements to facilitate the diffusion of health IT throughout the United States. These changes will help promote better outcomes for patients. Among the improvements are new Anti-kickback Safe Harbors and Stark Law exceptions; a study of, and subsequent authority to preempt some state privacy laws; and the replacement of ICD-9 diagnosis codes with ICD-10 codes.

Laboratories play a critical role in healthcare delivery by allowing for the rapid and timely utilization of health information by providers. Laboratories and the medical information they provide are the heart of the medical record. Laboratory data represent 60% of the medical record. Diagnostic tests comprise only 5 % of total hospital costs and only 1.6% of Medicare costs, but they influence a much larger portion (as much as 60-70%) of clinical decision-making that improves care and decreases cost. Virtually every health care community (i.e. Regional Health Information Organizations or RHIOs) that is trying to develop an electronic health information infrastructure is looking to laboratories first. A recent nationwide survey by the eHealth Initiative found that, of those who have electronic health information exchange efforts under way, 60% plan to exchange laboratory information within six months to support quality, safety and efficiency goals. In a survey of hospitals, the number one IT function in the majority of hospitals today is the electronic order entry and review of results for diagnostic services.

The reach of laboratories into physician offices and hospitals vis-à-vis the provision of this hardware and software has served as a 'catalyst' in the evolution of health IT. For example, Quest Diagnostics Incorporated, a member of ACLA, has business relationships with approximately half of the physicians and hospitals in the U.S. Quest Diagnostics Incorporated receives 40% of orders and sends 60% of its results via the internet. Similar means of laboratory connectivity are offered by other ACLA's other members.

The federal government, quality organizations, the Medicare Payment Advisory Commission (MedPAC) and others recognize that laboratory data are the essential building block for assessing quality care and will have a critical role in pay-for-quality initiatives. Laboratories can and have been used to measure a provider's performance as a critical component of health care delivery; however, this contribution cannot be realized without incurring additional cost that must be recognized and reimbursed. In a detailed study of practice and laboratory connectivity, the eHealth Initiative recently recommended incentives that could be provided for including electronic laboratory data as part of pay-for-performance reporting. One example from the report would be to provide short term incentives, based on the volume of laboratory messages processed, up to a monthly dollar limit per clinician that would encourage implementation of interfaces. Incentives such as these can be an important driver of adoption of new technologies. By providing incentives encouraging the transmission of laboratory test requisition and results reporting, the healthcare system will actually save money through reductions in duplicative testing, better coordinated care and decreases in morbidity and mortality.

Because of the value that laboratories convey in the data they transmit, they have pioneered the provision of secure, streamlined IT solutions to order and transmit laboratory tests. This is a critically important and highly valued function. So important that since 1995 laboratories have had a limited exception under the Stark Law to provide "items, devices, or supplies that are used solely to…order or communicate the results of tests or procedures for such entity."[1] This is a fundamental capability for laboratories to render services to providers and a critically important function that must be maintained. Clinicians place a high value on being able to order laboratory services and receive laboratory results electronically because it improves legibility, decreases error rates, produces more timely results (including STAT testing), and allows the monitoring of redundant or duplicative testing. The result is improved clinical outcomes, and improved clinical care efficiency with the long-term benefit of reduced healthcare costs.

We recognize physicians, hospitals and other providers routinely cite the fear of legal action/debarment from Medicare as one of the biggest deterrents towards adoption of health IT. Accordingly, HR 4157 establishes a new exemption for the provision of health IT and related training. ACLA believes this legislative proposal, if enacted, would help to address some of these concerns and prompt further adoption of the health IT; however, ACLA believes such an exemption should be crafted carefully to diffuse the technology while guarding against abuses. By doing so, providers will continue to compete on the services they are providing and not, for instance, the size of a monitor. However, in any law or regulation laboratories must be among those entities permitted to offer these items or services because of the critical role laboratories have, and continue to play in facilitating health IT adoption in the health care community. ACLA was particularly perplexed with HHS' Office of the Inspector General's recent notice on the establishment of new Stark Law exceptions and Anti-Kickback Safe Harbors which proposes to exclude laboratories from the newly created exemptions.

ACLA also supports the legislation's federal preemption of state laws that contradict the Stark Law exceptions and Anti-Kickback Safe Harbors established under the bill. Today, there are several states whose 'Stark' laws are complicated and have different requirements than the federal law. Similar to the privacy issue (which I'll talk about shortly), the problem is not just that these state laws are more stringent, but that there are many different standards. The differences in these state laws fall into several categories, e.g. the scope of the exceptions to the prohibition or the scope of what is considered a 'designated health service.' By creating a federal preemption, Congress can help address the fear and confusion many providers continue to have as they contemplate adoption of various health IT solutions.

Another of the much-needed changes that HR 4157 addresses is the need for federal preemption of state laws related to the security and confidentiality of health information. HR 4157 requires a study of: 1) the degree to which laws vary among the states; 2) between state laws and HIPAA; 3) how such variations adversely impact confidentiality and the electronic exchange of health information. Upon enactment, Congress will have three years to pass legislation establishing uniform federal standards and preempting state laws with regard to confidentiality and privacy. If not, then the Secretary of HHS is permitted to adopt regulations based on the results of the study.

ACLA supports this provision because the patchwork of state privacy laws is an impediment to health information exchange. For example, LabCorp, a large national laboratory, has been invited to participate in two of the eight regional Medicare Health Support pilot programs (previously known as the Chronic Care Improvement Program) authorized by section 721 of the Medicare Modernization Act. Chairman Deal, LabCorp has been invited to participate in an effort with CIGNA HealthCare in your home state of Georgia as well as a program operating in central Florida being operated by Green

[1] 42 USC 1395nn(h)(1)(C)

Ribbon Health, LLC. These entities will offer self-care guidance and support to chronically ill Medicare beneficiaries to help them manage their health, adhere to their physicians' plan of care, and ensure that they seek the medical care and Medicare-covered benefits that they need. LabCorp's role in the pilot programs would be to transmit laboratory data to CIGNA HealthCare and Green Ribbon Health for those beneficiaries who voluntarily participate in the program. This information would then be used to help monitor the conditions of participants and ultimately, improve their outcomes.

Unfortunately, despite the well-intended efforts of these programs, more restrictive state laws in Florida and Georgia governing the release of lab results have prevented LabCorp from transmitting these important results to Green Ribbon Health or CIGNA HealthCare until its concerns about the application of those laws to these requests have been addressed. More specifically, the Florida and Georgia laws preclude providing test results to anyone other than the ordering physician or provider (or to a person specifically authorized by the ordering physician). In this case, had there been a federal preemption of state laws we would be talking about the successes/failures of these program and not 'red tape.'

HR 4157 also addresses the needed replacement of the International Classification of Diseases, 9th edition, Clinical Modification (ICD-9-CM) diagnosis and procedure billing codes with ICD-10-CM/PCS codes. ICD diagnosis codes are used by inpatient and outpatient providers for billing and reimbursement. Under the Medicare program, laboratories are paid by including ICD-9 codes on their claims to provide medical necessity. These ICD-9 codes are provided by the physician to the laboratory and are subsequently attached to a claim and submitted to CMS. Today, as many laboratories will attest, problems persist with physicians not providing the appropriate ICD-9 codes in order for laboratories to get paid. Currently, ICD-9 provides approximately 13,000 diagnosis codes. Take into account that ICD-10 provides 120,000 diagnosis codes, and one can see the potential for massive delays in reimbursement for laboratories and many other providers and thus the need for an extended phase in of the new system.

To give you an example of the difference between ICD-9 and ICD-10 consider how a physician would document an accidental sports injury. Under ICD-9, a diagnosis of a sports injury caused by striking against or being struck requires a single code: E917.0, described as "Striking against or struck accidentally in sports without subsequent fall; includes kicked or stepped on during game (football, rugby), struck by hit or thrown ball, struck by hockey stick or puck. Under ICD-10, a similar diagnosis requires one of 24 codes, meaning that the physician must document the causation (see attachment).

ACLA recommends that the implementation period for the transition to ICD-10 be changed from a two-year phase in period to a five-year period. Doing so would provide adequate time to reprogram all health care providers' and payers' computer systems to accommodate the new, longer ICD-10 codes. In addition, considerable time and expense will also have to be spent on client education and testing of the new systems. During this 'transition period' it should be permissible for providers to bill using either the ICD-9 or ICD-10 standards.

In conclusion, ACLA supports the Health Information Technology Promotion Act's new Anti-kickback Safe Harbors and Stark Law exceptions, the bill's proposed preemption of some state privacy laws, and a replacement of the ICD-9 with ICD-10 with a five-year transition period.

I'd like to end on this note. It has been said that every effort in the health care public policy arena aims to improve three different aspects of health care: better, faster, and cheaper. Nothing to date has been able to meet all three objectives – some systems provide two of the three but always at the expense of the third. I believe health IT is the answer. Health IT will make health care better by improving outcomes; faster, by facilitating not only the delivery of information but the coordination of care; and cheaper,

by reducing the costs of doing business, be it a reduction in duplicative testing or by saving precious time previously spent on data entry.

Mr. Chairman, thank you for the opportunity to share ACLA's perspective on ways to promote electronic health records and a smarter health information system. We are ready to work with you on this important and vital legislation. If you have questions or need any additional information, please do not hesitate to contact us.

MR. DEAL. Thank you. Mr. Vaughan.

MR. VAUGHAN. Mr. Chairman, members of the committee, thank you for inviting us today. Consumers Union is the independent, non-profit publisher of Consumer Reports, and we do not just test toasters, we work on health issues, and had a large article on this topic in the March issue. We strongly support the movement toward electronic health records as a way to improve quality and moderate health costs.

But we believe that the American public will not fully support or fully use or fully benefit from the great potential of such systems unless more is done soon to ensure the privacy of medical information. As IBM's testimony just said, the privacy issues and the public's perceptions of those issues must be addressed in order for personal health records to succeed. Patients need meaningful control over their medical records, the right to keep their records private, and they should not be forced to give up privacy as a condition of treatment. We talk of consumer-directed healthcare, an ownership society, and personal empowerment. Mr. Shadegg was talking about choice. The right to privacy is the heart of all of that.

There must be a strong enforcement of privacy laws, and if privacy is violated, people should be notified of that breach and given a private right of action, as Georgia is one of the States that allows that. The State should have the right to enact privacy laws above and beyond HIPAA's terribly minimalist provisions in our opinion. Dr. Detmer's testimony has a neat point about how complex that could be, particularly if you look at Virginia, Maryland, and D.C. How would a computer keep track of all that? But rather than coming down to the Federal level, could we work with the governors and the State legislators to say what did the States feel they needed to do and see if there was a model law that we could come up to rather than come down.

Privacy needs to be strengthened, not weakened, and we urge you to oppose legislation that would preempt stronger State laws or let HHS bureaucrats weaken the Fourth Amendment. As we like to say, one size does not fit all, and this is the way we look at that. Attached are a set of consumer privacy principles on my statement that we hope you might look at as you consider legislation. Assuming we can get true privacy, we would like to see quick dissemination of good systems. We

recommend, however, against making broad exceptions to the anti-kickback and physician referral laws for donations.

Given the Federal budget situation, it is very understandable if people would look for a sort of free way to promote dissemination, like suspending these anti-fraud laws. We believe, however, that such action would have a very limited impact on the adoption of IT and would not be always good for consumers. This approach may not be free. It may have a cost. Basically there are no free lunches in life. I would bet you that Adam Smith would say most businesses do not give away something of value to another business unless they expect a return on the investment.

When a hospital system offers an IT package to doctors, it hopes the ease of communication between them and the goodwill generated by the gift will encourage referrals, regardless of whether that facility is the best quality or value facility for the patient. There is a parallel example in an area we know that causes higher and more costly utilization. Why do pharmaceutical companies give away free drug samples? It is because in our culture the act of giving a gift, even a trinket, conveys a psychological sense of obligation, I owe you one. That is human nature. In the case of free drugs, it leads to higher utilization and high costs products.

So please be skeptical. Companies, many for profit, who spend 98 percent of the year telling Congress they are not paid enough by Medicare and Medicaid, they are all going broke, they have found some money that they now want to donate to a bunch of small businessmen making about $160,000 a year, who are very smart businessmen, but have not been smart enough to realize they need to move to IT. It is kind of strange. I think it would increase care coordination under the right situation, but please be careful in how you draft this.

We think there are better ways to encourage more adoption of IT that do not weaken the anti-fraud laws. For example, you might explore with CBO whether, as you fix the Medicare doctor payment system in a budget neutral, time-limited way you could voluntarily encourage physicians to install certified IT by adjusting the practice expense payment and then collect it back at the end of the five-year cycle. It might be tough but worth talking to CBO about. Representative Murphy's bill kind of gets into that a little bit in section 8.

In conclusion, these anti-fraud laws are very delicate things, and we hope you will be careful, as I know you will be. Thank you, sir.

[The prepared statement of Bill Vaughan follows:]

PREPARED STATEMENT OF BILL VAUGHAN, SENIOR POLICY ANALYST, CONSUMER'S UNION

Mr. Chairman, Members of the Committee:

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

The Potential

We strongly support the movement toward electronic systems of health records (EHR) and information exchange. By harnessing the power of modern information technology systems we can improve the quality of American health care and moderate health costs by:

- reducing errors,
- eliminating service duplication,
- promoting pay-for-performance, and
- providing the data necessary to evaluate the true comparative effectiveness of various treatments and drugs.

As just one example of the tremendous improvements in quality and cost savings that are possible, Consumers Union has been conducting a national campaign to promote the disclosure of hospital infection rates (www.StopHospitalInfections.org). Each year, there are about 2 million patients who acquire infections in hospitals, and about 90,000 die. The increased cost to the health care sector is in the tens of billions of dollars. We have been working at the state level to pass laws to require hospitals to report their rate of infection in the belief that public disclosure will prompt hospitals to adopt effective methods to reduce their infection rates. Electronic medical records technology and the public disclosure of more types of de-identified patient care data will make it easier for consumers to reward those who provide quality.

The Critical Need to Ensure Privacy

While there can be important public and private benefits of creating an effective electronic medical records system, we believe (and polls demonstrate[1]) that the American public will <u>not</u> support, fully use, or benefit[2] from the great potential of such systems unless more is done—now--to ensure the privacy, security, and appropriate use of medical information. This requires enabling patients to decide when, with whom, and to what extent their medical information is shared. As Dr. David Brailer, head of the Office of the National Coordinator for Health Information Technology, responded March 3 to a letter (see Attachment #1) from consumer groups, "we will achieve our goal of widespread [EHR] adoption only if patients are confident that their health information is private and secure." Today, it is not private or secure.

This concern should especially resonate with public officials such as you, who are so subject to prying eyes and gossiping tongues.[3] I think we all have to admit that there is no hack-proof database or system. Once our medical data is moving electronically, it is

---

[1] See as just one example Caroline Broder, "Survey: Consumers Concerned About Control, Access to Medical Info," *Healthcare IT-News*, January 18, 2006.

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

[3] Testimony of Joy Pitts, Assistant Research Professor, Georgetown University, July 27, 2005 before the Ways and Means Health Subcommittee, citing the Rep. Velasquez and former President Clinton examples, page 2. See also Robert Dallek's <u>An Unfinished Life</u> (p. 261ff) for a description of LBJ's efforts to obtain medical information on JFK and how Kennedy avoided certain important medical tests so as not to have a medical record.

subject to threats from hackers, identity thieves and others. That is simply a fact of life, re-confirmed almost daily by new stories of financial and medical record data violations.[4] Beyond the likely scenarios of security breaches, the value of electronic health information is such that many organizations will want to exploit secondary data sources for private financial gain, rarely (if ever) with patient knowledge, let alone consent.

So what can we do to minimize concerns and improve privacy in electronic health records?

The American public needs to be given meaningful control over their medical records. That means they must have a right to keep their records private and that they cannot be forced to give up control of their most private medical information as a condition of treatment.

The penalties for violations of privacy are inadequate and have major gaps.[5] There must be strong enforcement of privacy and security laws, and if a person's privacy is compromised or violated, they should be notified of that breach and have a private right of action.

The States should have the right to enact privacy laws above and beyond HIPAA's absolutely minimal provisions and that right must not be pre-empted. Privacy needs to be strengthened, not weakened, and we urge you to oppose legislation that would pre-empt stronger State laws or delegate to the Secretary of HHS authority to pre-empt such laws. These State laws offer extra protection and peace of mind to patients with mental health, STD, cancer and other treatment issues. As 30 organizations in the Mental Health Liaison Group wrote Congress on November 15, 2005, adding improved privacy protections to proposed EHR bills is essential in the mental health sector.[6]

Some will say that it is too complex or too expensive to allow people to control their medical information. But that's why computers are so wonderful! They can be designed to deal with huge numbers of variables—like 50 state laws-- and to create special files where certain data (such as a mental health record) is only available to a designated provider on a "need to know basis." If we do not meaningfully address the privacy issue, polls show the public will not trust this system, many will go to a medical underground 'off-the-books'[7], and we will just increase public cynicism about big government and big business controlling our lives. In an age when the talk is of consumer driven health care, and ownership, and empowerment, forcing people to share their most secret personal medical information is not the path to take.

Attached are a set of consumer principles that was developed under the leadership of the National Partnership for Women & Families and that Consumers Union, AARP, and seventeen other groups are supporting.[8] We urge you to include these principles in whatever legislation you may develop.

---

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

[5] Joy Pitts, op. cit., p. 4.

[6] See letter from National organizations representing consumers, family members, advocates, professionals and providers, c/o Peter Newbould, American Psychological Association Practice Organization, 750 First Street, NE, Washington, DC 20002.

[7] Reportedly millions of Americans already forgo sensitive treatments because of privacy concerns. 65 Federal Register 82,778.

Oppose Incentives to Promote Technology Give-Aways that may Distort Health Care Delivery

Assuming true privacy and increased security, we all would like to promote the fastest possible movement to EHRs and a 'networked' health care system so as to benefit from the quality and cost savings potentials. We recommend, however, against making blanket exceptions to the anti-kickback and physician referral laws for donations of EHR systems.

Given the Federal budget situation, it is understandable that some are attracted by the idea that such blanket exceptions might be a 'free' ways to promote EHR technology dissemination. We believe, however, that such action would have a very limited impact on the adoption of EHR systems and would not be good for consumers. This approach is not free—it has a cost, as we describe below.

Most businesses don't give away something of value to another businessperson unless they expect a return on the investment. When a hospital system offers an IT package to a non-affiliated physician group, it hopes the ease of communication between them (and the goodwill generated by the gift) will encourage referrals to its facilities, regardless of whether that facility is the best quality or value facility for the patient.

There is a parallel example in an area we know causes higher and more costly utilization: Why do pharmaceutical companies give free drug samples (and pens and pads of paper, etc., etc.) to doctors? Because in our society and culture, the act of giving a gift, even a trinket, conveys a psychological sense of obligation—"I owe you one." That is human nature. In the case of 'free' drugs, it leads to increased utilization of high cost products. That is what the anti-kickback and physician referral rules tried to deal with: the act of giving something of value creates "ties" that cause referrals and utilization to go up, without regard to need, cost, or quality.

It is worth spending a minute more on the 'free' drug example. There has been a great deal of concern about the way drugs are promoted and the impact that has on costs and quality of care. The January 25, 2006 issue of JAMA (Vol. 295, No. 4, p. 429ff) carried an article by some of America's most distinguished physicians entitled, "Health Industry Practices That Create Conflicts of Interest: A Policy Proposal for Academic Medical Centers," that calls on the nation's teaching hospitals to lead an ethical revolution and reject all industry gifts, since those gifts distort the practice and integrity of medicine. As the doctors wrote:

> Social science research demonstrates that the impulse to reciprocate for even small gifts is a powerful influence on people's behavior. Individuals receiving gifts are often unable to remain objective: they reweigh information and choices in light of the gift. So too, those people who give or accept gifts with no explicit "strings attached" still carry an expectation of some kind of reciprocity. Indeed, researchers suggest that the expectation of reciprocity may be the primary motive for gift-giving.
>
> Researchers have specifically studied industry gifts to physicians. Receiving gifts is associated with positive physician attitudes toward pharmaceutical representatives. Physicians who request additions to hospital drug formularies are far more likely to have accepted free meals or travel funds from drug manufacturers. The rate of drug prescriptions by physicians increases substantially after they see sales representatives, attend company-supported symposia, or accept samples. The systematic review of the medical literature on gifting by Wazana

found that an overwhelming majority of interactions had negative results on clinical care.[9]

If medical practice is distorted by the relatively small value of drug company gifts, imagine the consequences of large EHR technology "gifts"!

What if Congress proposed (though it would not take a law) that companies and providers could give money or equipment to a truly neutral charity in an area (for example, the Red Cross, the American Public Health Association, a State Medicaid Agency) that would then distribute the gift on some basis of need and there would be no tie between the donor and the recipient? I think most potential donors would find lots of reasons why that wouldn't work. And that should tell you everything: the donor wants a "tie" with the recipient that will result in goodwill and increased referrals. For consumers, the problem is that the "tie" and resulting increased referrals may not be the best for the patient because the donor may not be the best or lowest-cost provider in an area. And donors who have the resources to give may just increase their economic dominance in an area, thus reducing future competition and driving up costs.

Look for real solutions to speeding dissemination of IT

There are better ways to encourage more adoption of EHRs. Once progress is made on technology and process standards and there is more agreement on the best hardware and software paths, Congress may want to promote the dissemination of such technology and pay for it in a way that does not distort practice patterns. You might explore with CBO whether, as you try to fix the Medicare physician payment system (SGR), a budget neutral, time-limited way to encourage physician installation of certified EHR could be possible. For example, would CBO score as neutral a system where on a voluntary basis, a physician could greatly increase their practice expense payments for several years so they could more easily finance the installation of a 'certified' EHR system. Then in the next several years they would repay that 'advanced' amount through reduced practice expense payments, on the grounds that the installation of the equipment will reduce paperwork and clerical practice expense in future years. Another encouragement to take advantage of this opportunity would be a requirement that by a date certain all Medicare-Medicaid EHRs would have to be through certified systems.

Congress could also help providers in the future by using the certification process to obtain a discount price for EHR hardware and software.

In summary, we urge you to consider alternatives to encouraging the dissemination of this new generation of equipment in ways that do not weaken the nation's anti-fraud laws.

If Congress feels compelled to proceed with anti-kickback and anti-referral law changes, we urge you to consider limited exceptions based on modifications to the Administration's October 2005 proposed regulations.

These draft regulations would permit exceptions—but not blanket exemptions--to the anti-kickback and physician referral laws for EHR donations. Consumers Union, the National Partnership for Women & Families, and five other national organizations filed

---

[9] Eleven footnote references to sources for statements omitted from quote. For a less scholarly description, see "The Drug Pushers, by Carl Elliott, MD, Ph'D in The Atlantic Monthly, April, 2006: "After awhile even the most steel-willed doctors may look forward to visits by a [drug] rep, if only in the self-interested way that they look forward to the UPS truck pulling up in their driveway. A rep at the door means a delivery has arrived: take-out for the staff, trinkets for the kids, and, most indispensably, drug samples on the house. Although samples are the single largest marketing expense for the drug industry, they pay handsome dividends: doctors who accept samples of a drug are far more likely to prescribe that drug later on. Such gifts do not come with an explicit quid pro quo, of course. Whatever obligation doctors feel to write scripts for a rep's products usually comes from the general sense of reciprocity implied by the ritual of gift-giving."

formal comments expressing serious concern about the exceptions and urging major changes (see attachment #2).

For example, we recommend changing the regulations to:

--delay the effective date of the exceptions until the product certification process for ambulatory care that the Administration is now aggressively supporting is in place (otherwise you encourage donations that may lead to technological dead-ends and wasted time and effort—e.g., Beta v. VHS competing donations);

--limit the exception to donations to physicians or clinics that provide a certain level of uncompensated charity care or serve a significant number of Medicaid patients; or if that is not possible, require donors to offer the technology to all (their) physicians, not just those who provide high volumes of profitable business;

--sunset the exemptions;

--require recipients to copay a portion of the cost: totally free equipment is likely to sit in the closet. The equipment needs to be something that the recipient wants enough to put some of his own resources into.

Thank you all for your time and attention.

Attachment #1

Health Information Technology – Consumer Principles
March 2006

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

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

Principles

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

- Individuals should have a means of direct, secure access to their electronic health information that does not require physician or institutional mediation.
- Individuals should have access to all electronic records pertaining to themselves (except in cases of danger to the patient or another person).

- Individuals should be able to supplement, request correction of, and share their personally identifiable health information without unreasonable fees or burdensome processes.

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

- Individuals should receive easily understood information identifying the types of entities with access to their personal health information and all the ways it may be used or shared. The explanation should include any sharing for purposes other than the immediate care of the individual, and should explicitly identify intentions for data use such as public health protection, quality improvement, prevention of medical errors, medical research or commercial purposes.
- Access to personal health information must be limited to authorized individuals or entities.
- Tracking and audit trail systems should be in place that permit individuals to review which entities have entered, accessed, modified and/or transmitted any of their personally identifiable health information.

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

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

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

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

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

- Independent bodies, accountable to the public, should oversee electronic health information sharing.

- Consumers should have equal footing with other stakeholders.

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

Implementation of any regional or national electronic health information network should be accompanied by a significant consumer education program so that people understand how the network will operate, what information will and will not be available on the network, the value of the network, its privacy and security protections, how to participate in it, and the rights, benefits and remedies afforded to them. These efforts should include outreach to those without health insurance coverage.

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

Attachment #2

Comments of Groups on HHS Proposed Regulations on anti-kickback and physician referral[10]

Comments on Office of the Inspector General Proposed Rule OIG-405-P

As organizations representing a wide range of consumer interests, we are pleased to have the opportunity to comment on the proposed rule OIG-405-P that would add a new paragraph (x) to the existing safe harbor regulations at 42 CFR 1001.952. The proposed safe harbor would protect donation of specific items and services for prescribing drugs electronically. The preamble to the regulations also describes the scope of two planned additional safe harbors for electronic health records software and directly-related training services, but the Office has not proposed actual regulatory language for such a safe harbor.

[10] This is the comment on anti-kickback proposed rule. Basically identical comments were filed on CMS-1303-P, relating to the physician referral proposed rule.

We recognize the potential of health information technology (HIT) to improve health care quality. Furthermore, we support efforts by the Department to promote the use of HIT by physicians and other health care providers, and are encouraged by the prospect of reduced errors and higher quality if e-prescribing is implemented. Below are our comments on the proposed safe harbor.

Pre-interoperability Electronic Health Records Safe Harbor

The Office is considering the creation of a safe harbor for donations of electronic health record technology made prior to the adoption of product certification criteria by the Secretary. We oppose this provision and recommend it not be included in the final regulations.

The Department is moving aggressively to put product certification criteria for ambulatory care in place in 2006. Promoting investment in this technology before DHHS adopts those criteria may seriously impede reaching the goal of a common platform – a goal which is part of the rationale for making this safe harbor. Furthermore, allowing the safe harbor to be in effect prior to certification could encourage providers and manufacturers to press for delay in adoption of the certification standards in order to avoid having to make new investments or to retain the market advantages they have created by installing their systems in physician offices.

Post-interoperability Electronic Health Records Safe Harbor

In a parallel proposed rule, CMS-1303-P, the Department has included the actual text of a proposed regulation to provide an exception to the Stark statute for donations of electronic health records software if the donation is made after the product certification criteria are adopted and if the software is compliant with the certification requirements. We support the intent of this exception but have some concerns about some of the text; we have outlined our concerns in comments filed today on CMS-1303-P. The Office has asked for comments on its plans for a similar safe harbor, described in section II.B.2 of proposed OIG-405-P. Our comments on the potential safe harbor are similar to those expressed with regard to the Stark exception. For convenience, our views are set forth below in the context of the proposed CMS Stark exception text.

Subsection §411.357(x)(4) [of CMS 1303-P] requires that neither the selection of the physician nor the amount or nature of the items and services donated can turn on the volume or value of referrals or other business generated between donor and recipient. The section then enumerates six specific criteria that a donor might use that would be deemed compliant with the exception requirements:

1) total volume of prescriptions the recipient writes;
2) size of the medical practice;
3) number of hours the physician practices medicine;
4) extent of use of automated technology in the recipient's medical practice;
5) if the donor is a hospital, whether the physician is on its staff; or
6) another method that "is based on any reasonable and verifiable manner that is not directly related to the volume or value of referrals or other business generated between the parties."

This section is the heart of the proposed rule. The widespread adoption of EHR and EP technology can bring great benefits to patients, providers and insurers. Health information technology can help reduce medical errors, encourage patient activation and adherence to recommended regimens, and provide tools to evaluate clinical effectiveness, population health status, and the quality of medical care. The drive to promote the wider use of EHR and EP technology should not, however, trump the consumer protection or program integrity brought by the antifraud and abuse prohibitions. Donors should not be allowed to selectively fund physicians based on the volume of their prescribing, size of practice, or whether they are likely to be high users of technology since these could be

proxies for the generation of referrals and revenue. We therefore recommend the following changes:

––Eliminate item #6, above. It is too open-ended and subjective and could become a major loophole.

––Our preference would be to require that donors offer the technology to all their physicians. In the case of hospitals that would be all physicians with privileges; for MCOs, all physicians in the MCO network; for group practices, all physicians in the group. In the case of an MCO, where it might be impractical to include all network participants, donors could be permitted to give priority to those physicians or clinics that have a certain percentage of their patients in the MCO. Similarly, for hospitals the alternative might be all physicians with privileges of a general category such as: a) practice privileges, or b) admitting privileges.

––Add a new exception that permits the donation to a physician or clinic that provides a certain level of uncompensated charity care or a combination of charity care and Medicaid patients. It is these providers – the community clinics, solo practitioners in rural communities or medically underserved areas – who are least likely to have the resources to make the health information technology investments on their own.

In the preamble to the proposed regulations the Department asks for comments on a cap on the value of the EHR donation, either a maximum percentage of the value of the technology (which would require the physician to share the costs) or the lower of a fixed dollar amount or the percentage of value. We believe it would be hard to use a fixed dollar amount cap. The cost of technology will change over time and vary depending on the nature of the system. A cap on the percentage of the value of the technology being donated appears to be the more viable option. The physicians or clinics with high Medicaid and/or charity care caseloads should be exempted from cost-sharing.

Subsection 417.357(x)(9). This subsection requires that any donated EHR software contain electronic prescribing capability that complies with the electronic prescription drug program standards under Medicare Part D at the time the items and services are furnished. In the preamble the Department states that it "wants to ensure that integrated packages that could positively impact patient care are not excluded from the postinteroperability exception." We support the development of software in ways that promote avoidance of medical errors, improve quality of care, and/or enhance public health preparedness. It would be desirable that, as the Secretary adopts additional standards for EP, and for EMR systems, any donations qualifying for this exemption also have to comply with those standards without the necessity that the Department amend these regulations. We suggest the Department consider that possibility in shaping the final regulations.

Sunset section 411.357(x) entirely at a designated date. The rationale for allowing an exception to antifraud prohibitions decreases with the passage of time. Physicians may not purchase EHR technology now, but in the future having such technology will be a standard and necessary part of medical practice. At that point there will be no need for third parties to donate such technology. Furthermore, if interoperability becomes the norm, incompatibility across a network of providers ceases to be an issue. We therefore strongly urge that this entire section authorizing the Stark law exception for EHR be eliminated not later than five years from the date of publication of the final regulations. Alternatively, the sunset date could be delayed for up to two additional years if the Secretary makes an administrative finding that there is still a need for the exception to promote adoption of EHR technology.

While we support some limited exceptions to the physician self-referral prohibition, and the creation of additional safe harbors under the Anti-Kickback statute, for donations of EP and EHR technology, we believe these exceptions will have only a modest impact

on the expansion of their use. Of much more importance are the standards harmonization and product certification efforts the Department already has underway. Equally important will be direct funding of loans and grants to states and providers and financial incentives for the adoption of HIT being incorporated in federally supported health care programs, including Medicare, Medicaid, FEHBP, TriCare, and SCHIP.

Thank you for considering our comments.

National Partnership for Women & Families
AFL-CIO
American Federation of State, Federal and Municipal Employees
Consumers Union
Department for Professional Employees, AFL-CIO
National Consumers League
Service Employees International Union

MR. DEAL. Thank you. Mr. Neaman.

MR. NEAMAN. Chairman Deal and members of the subcommittee, good afternoon. On behalf of the Healthcare Leadership Council, thank you for the opportunity to testify before you this afternoon on the importance of health information technology and some of the important steps that need to be taken to create a national health information network. I am here this afternoon wearing two hats, first as the Chairman of the Healthcare Leadership Council, a coalition of many of the Nation's leading healthcare companies and organizations. The HLC has a longstanding interest in this issue and shares the President's and this Congress' commitment to achieving widespread adoption of health information technology.

I am also here today speaking as the President and Chief Executive Officer of Evanston Northwestern Healthcare, a large academic medical center in northern Illinois comprised of three hospitals, a 500-physician multi-specialty group practice, and a medical research institute that has over $100 million of NIH grants. At our organization the dream of electronic medical records is no longer a dream. It is a reality across all three of our hospitals and over 70 of our doctor offices and clinics. We have had a full electronic medical record up and running for over two years, and I can tell you that it is powerful and transformational and really makes a difference in the quality of care and the reduction of medical errors, improvement of life for our nurses and our pharmacists and our staff, and improving the efficiency for all consumers.

In 2003 we launched the EPIC comprehensive electronic medical records system that indeed provides all of our hospitals and physicians with a single, legible, unified source of clinical information. The healthcare professionals at Evanston can tell you firsthand, and with great confidence, that health information technology can and must transform our Nation's healthcare system for the better. We have been able to deliver medications to patients faster. We have significantly

reduced medical errors, and in one specific example when the manufacturer of Vioxx took the drug out of commission, we were able to communicate and identify over 2,000 patients on the drug, communicate with their physicians and the patients, and make changes to this drug in three hours. That would be impossible to achieve with paper records.

The task before us is to make sure that this capability is available to all patients in the United States through interoperable electronic health records, and today I would like to highlight three challenges that must be met in order to achieve this goal. First, we have to have a multi-State interoperable health information system that must have uniform Federal standard governing patient privacy. Our current confidentiality framework rests upon literally thousands of State statutes, regulations, common law principles, and advisories. Not only do States differ from each other on their privacy rules, but virtually no State requirement is identical to the Federal HIPAA privacy regulation. This checkerboard of varying rules would definitely stand in the way of an interoperable multi-State information network.

To address this problem, we urge Congress to act on H.R. 4157, the Health Information Technology Promotion Act of 2005, which is co-sponsored by several members of this subcommittee. This bill establishes a process to ensure a uniform national standards is achieved that preserves and protects the security and confidentiality of patient health information. We believe this legislation is critical to achieving the Nation's HIT objectives. Another challenge we face concerns HIT financing. Developing the EPIC system at Evanston Northwestern Healthcare required over $40 million of investment and our operating expenses initially went up by over $5 million per year to make sure that the system runs and runs well.

Many healthcare providers, I would suggest most, do not have the capital on hand to make this kind of investment, not only in our hospitals but certainly in our physician offices. We believe that is in the Nation's interest, given the importance of interoperable HIT to patient safety and the Nation's emergency preparedness to drive implementation through financial incentives and creative funding mechanisms, and we are prepared to work to help you shape such an initiative. Finally, we believe that greater physician adoption is essential for electronic health records to occur in our hospitals and medical groups and to occur well.

This will lead to greater integration of physician and hospital information systems that will result in better quality of care for patients and saved lives. For this to happen though, Congress needs to provide exceptions to the current physician's self referral prohibitions and anti-kickback rules that were not intended to prohibit the kind of beneficial patient-centered actions we are discussing today. Let me close, Mr.

Chairman, by again thanking the subcommittee for spotlighting the vital importance of these issues. We look forward to working with you in the months ahead to bring advances in technology closer to the patients and families that we are privileged to serve, and we would be very pleased to address your questions. Thank you.

[The prepared statement of Mark Neaman follows:]

PREPARED STATEMENT OF MARK NEAMAN, PRESIDENT AND CEO, EVANSTON NORTHWESTERN HEALTHCARE, ON BEHALF OF HEALTHCARE LEADERSHIP COUNCIL

Chairman Deal and Members of the Subcommittee, I want to thank you on behalf of the members of the Healthcare Leadership Council (HLC) for the opportunity to testify on legislative proposals that will promote electronic health records and a smarter health information system.

My name is Mark Neaman and I am president and CEO of Evanston Northwestern Healthcare of Evanston, Illinois. We are an academic health center connected with Northwestern University, comprised of three hospitals, a 463-physician medical group, a home health services agency and a medical research institute.

My interest in coming before you today is twofold. First, I am chairman of the Healthcare Leadership Council (HLC), a not-for-profit membership organization comprised of chief executives of the nation's leading health care companies and organizations. Fostering innovation and constantly improving the affordability and quality of American health care are the goals uniting HLC members. Members of HLC – hospitals, health plans, pharmaceutical companies, medical device manufacturers, biotech firms, health product distributors, pharmacies and academic medical centers – envision a quality driven system built upon the strengths of the private sector.

More to the point, the Healthcare Leadership Council shares President Bush's goal that most Americans have electronic health records by 2014. And we appreciate the bi-partisan commitment by Congress to encourage widespread adoption of health information technology.

I'm also here to share my own institution's experiences with health information technology. In July of 2001, the Board of Directors of Evanston Northwestern Healthcare gave the go-ahead to design and implement a patient-centric electronic health record system, a system that we call EPIC. Our goal was to utilize health information technology in a way that would improve clinical outcomes, enhance patient safety, provide greater patient satisfaction, and create a better working environment for our system's health care professionals.

I can testify, from our own experience, that all of the discussion about the promise of health information technology is not hyperbole. It is quite real. Let me give you some examples.

EPIC was launched in our Medical Group offices in January 2003 and then introduced incrementally in our hospitals over the next 12 months. We now have, throughout our three hospitals and all of our physician offices, a single, unified source of clinical information. With this accessible, comprehensive database, we have cut in half the amount of time it takes to deliver the first dose of an antibiotic to an inpatient, because of the speed with which we can check the possibility of conflicting medications or allergic reactions. In one year, we reduced by 20 percent the number of reported medication errors.

I think it would be useful for the committee to hear of a particular anecdotal benefit of the EPIC system. When the drug Vioxx was pulled from usage by the drug's manufacturer, we were able to use the EPIC system to remove the drug from our hospitals and physician offices, block future orders, send notices to physicians regarding

which of their patients were on the drug, and send electronic links to websites with information on Vioxx substitutes. This process affected over 2,000 patients and was completed in just three hours. To undertake this same task manually, utilizing paper records to try to find which patients were taking Vioxx, would have taken days if not weeks.

It is important to note that Health Information Technology is not just limited to electronic medical records, it also includes integrated medication delivery systems that reduce bedside intravenous medication delivery errors and the resultant harm to the patient. These state-of-the-art systems enable communication between doctors, patients, and pharmacies to ensure that the proper patient is receiving the proper drug in the proper dosage after the proper precautions were taken.

The Healthcare Leadership Council has such a strong interest in this issue because we've seen firsthand what widespread adoption of HIT can mean for patients and health care providers. Several HLC member organizations have been among the earliest adopters and pioneers of health information technology. We believe HIT has the power to transform our health care system and provide increased efficiencies in delivering health care; contribute to greater patient safety and better patient care; and achieve clinical and business process improvements.

Our interest in this issue is long-standing. In the summer of 2003, HLC established a Technical Advisory Board, comprised of clinicians and others with information technology expertise within HLC's member companies to provide information about their HIT implementation experiences.

Attached to my testimony is a copy of the White Paper that resulted from this effort. The paper attempted to quantify key benefits of HIT along with barriers to HIT implementation. The paper concluded with the following recommendations:

- Standards to assure interoperability;
- Financial incentives and funding mechanisms;
- Liability protections to facilitate sharing of safety and quality data; and
- Stakeholder collaboration on best practices.

In looking at these recommendations, it is clear that there has been significant progress since 2004.

Last summer, the President signed into law the, "Patient Safety and Quality Improvement Act." HLC advocated for this legislation as an important step toward fostering a culture of safety – through liability protections to allow voluntary information-sharing and reporting. I thank the Subcommittee members for all of your work to enact this important legislation.

In the area of standards, several public and private sector initiatives are making great strides to identify or develop health information interoperability standards that will enable disparate systems to "speak the same language." And the work of the Certification Commission for Health Information Technology will complement these efforts by certifying that products are compliant with criteria for functionality, interoperability and security. This will help reduce provider investment risks and improve user satisfaction.

As important as it is to applaud the progress that has been made, it is necessary to focus on the barriers that stand in the way of widespread HIT implementation. We have some significant challenges ahead of us, and I'll begin by discussing patient privacy regulations and standards.

Developing a multi-state, interoperable system depends on national technical standards as well as national uniform standards for confidentiality and security. The Health Insurance Portability and Accountability Act (HIPAA) governs the privacy and security of medical information. Though HIPAA established federal privacy and security standards, it permits significant state variations that create serious impediments to

interoperable electronic health records, particularly when patient information must be sent across state lines.

We believe Congressional action to establish a uniform federal privacy standard is essential in order to ensure the viability of a national health information network.

Because the HIPAA Privacy Rule's preemption standard permits significant state variation, providers, clearinghouses and health plans are required to comply with the federal law as well as many state privacy restrictions that differ to some degree from the HIPAA privacy rule.

State health privacy protections vary widely and are found in thousands of statutes, regulations, common law principles and advisories. Health information privacy protections can be found in a state's health code as well as its laws and regulations governing criminal procedure, social welfare, domestic relations, evidence, public health, revenue and taxation, human resources, consumer affairs, probate and many others. Virtually no state requirement is identical to the federal rule.

HLC is not alone in calling for action in this area. The 11 member Commission on Systemic Interoperability, authorized by the Medicare Prescription Drug, Modernization, and Improvement Act to develop recommendations on HIT implementation and adoption, recommended that Congress authorize the Secretary of HHS to develop a uniform federal health information privacy standard for the nation, based on HIPAA and preempting state privacy laws, in order to enable data interoperability throughout the country.

H.R. 4157, the "Health Information Technology Promotion Act of 2005," which several Members of the Subcommittee have cosponsored, anticipates and addresses this need.

The bill sets forth a process by which the Secretary of HHS develops a uniform standard for privacy laws. The bill does not simply adopt HIPAA "as is." Rather, the legislation requires the Secretary to conduct a study of state and federal security and confidentiality laws to determine the degree of variance and how such variation adversely impacts the privacy and security of health information as well as the strengths and weaknesses of such laws.

The Secretary then submits a report to Congress including a determination as to whether state and federal security and confidentiality laws should be conformed to create a single set of national standards; and what such standards should be. If the Secretary determines that a single federal standard is necessary and Congress does not act to create a standard in three years, the HIPAA privacy regulation, as modified by the Secretary based on the results of the study, will become the national standard. We believe that this legislation is critical to achieve our critical HIT objectives.

Since 1996, HLC has led the Confidentiality Coalition, a broad-based group of organizations who support workable national uniform privacy standards. The Confidentiality Coalition includes over 100 physician specialty and subspecialty groups, nurses, pharmacists, employers, hospitals, nursing homes, biotechnology researchers, health plans, pharmaceutical benefit management and pharmaceutical companies.

Many organizations and companies that are members or supporters of the Confidentiality Coalition sent a letter to Chairman Deal in support of a national standard for privacy and the provisions of H.R. 4157 that lay the groundwork for developing such a standard.

In discussing this issue, let me make one point abundantly clear. While we believe strongly in the need for a national privacy standard, HLC believes just as strongly that any regional or national system designed to facilitate the sharing of electronic health information must protect the confidentiality of patient information.

Health care providers and others involved in health care operations have appointed privacy officers, adopted compliance plans and conducted training with their employees to assure patients that they will protect their privacy in accordance with the HIPPA privacy rule.

Addressing this issue appropriately will be essential to achieving the interoperability necessary to improve the quality and cost effectiveness of the health care system – while still assuring patients' confidence that their information will be kept private.

To further underscore the importance of this issue to HIT development, I have attached to my testimony a map developed by the Indiana Network for Patient Care. Each dot represents a patient seen at an Indianapolis hospital during a six month period. While the dots are stacked very deep around Indianapolis as you would expect, patients served by the Indiana health providers during this period were also located in 48 of the 50 states. Today's health care providers, meeting the needs of a mobile society, serve patients from multiple and far-flung jurisdictions. Looking at this map it is easy to see why regional agreements will not be adequate to address the myriad regulations with which providers and others will need to comply to achieve "interoperability."

In addition to national privacy standards, the lack of funding or adequate resources – combined with the high costs of HIT systems – was repeatedly cited in our member study as a barrier to effective implementation of HIT systems. There are significant front-end and ongoing maintenance and operational costs for HIT, including software, hardware, training, upgrades, and maintenance. Systems are virtually unaffordable for those providers who do not have ready access to the operating capital needed for such an investment.

Developing the EPIC system at Evanston Northwestern Healthcare required hard capital costs of $35 million. This does not include an additional $7.5 million for consultants to write code for the system and undertake other essential tasks. Furthermore, our annual operating costs are increased by $5.5 million to support additional IT staff, training and software maintenance agreements.

In an age in which health care providers, in many cases, must deal with rising costs associated with uncompensated care, medical liability rates, homeland security needs and addressing staffing shortages, it is a simple fact that many providers do not have the financial wherewithal to invest in these new systems.

HLC believes that the federal government should drive the nation's implementation of HIT through financial incentives and funding mechanisms to help providers defray the huge costs of acquiring and operating HIT. Rapid implementation of interoperable HIT is also a critical component of the nation's emergency preparedness.

While the Agency for Healthcare Research and Quality (AHRQ) and Office of the National Coordinator for Health Information Technology (ONC) contracts and grants will support the development of a national information network and interoperability standards, we need to do more to get every provider using electronic health records now.

HLC advocates the consideration and implementation of multiple HIT funding mechanisms. However, we also recognize that current fiscal deficits and budget constraints will limit the ability of Congress to directly fund any new program or initiative. HLC is working with the chief financial officers of our member companies and organizations to develop workable, creative financing proposals for HIT. We look forward to sharing those ideas with the subcommittee.

There is one other critical issue I need to address today. One way Congress can facilitate greater physician adoption of electronic health records is to allow hospitals and medical groups that have successfully implemented electronic health records to share their expertise and IT investment with physician offices. This will facilitate better integration of hospital and physician information systems to improve continuity of care, decrease duplicate tests and provide greater safety and quality of care to consumers. By providing exceptions to the physician self-referral prohibition (Stark) and anti-kickback rules for HIT, Congress can accelerate physician use of electronic health records.

Current law prohibits anyone who knowingly and willfully receives or pays anything of value to influence the referral of federal health care program business, including Medicare and Medicaid. Physicians are also prohibited from ordering designated health

services for Medicare patients from entities with which the physician has a financial relationship – including compensation arrangements. The penalties for violating Stark and anti-kickback rules are significant. The Stark law is a "strict liability" statute and no element of intent is required. Violators are subject to significant civil monetary penalties and risk being excluded from participation in the Medicare and Medicaid programs. The anti-kickback law is a criminal statute that also provides significant penalties – including fines and imprisonment – for knowing and willful violations.

Though HHS has released proposed regulations that would provide limited exceptions to the Stark and anti-kickback rules for e-prescribing and electronic health records, industry analysis suggests that the exceptions will be of little value to hospitals and medical groups wanting to assist physicians with the adoption of HIT because they are too restrictive and contain overly burdensome requirements on donors and recipients of IT products.

Due to the severe consequences of violating these laws, providers need a workable safe harbor for HIT. Congress must provide a clear roadmap for hospitals, medical groups and others to provide HIT hardware, software, and related training maintenance and support services to physicians.

Pending legislation, such as H.R. 4157, establishes a safe harbor to the anti-kickback and physician self-referral rules for the provision of health information technology and related training services to health professionals.

Under the safe harbor, non-monetary remuneration in the form of HIT and training services is allowable if the remuneration is made without conditions that limit the use of HIT to services provided by physicians to individuals receiving services at the entity; restrict the use of HIT in conjunction with other HIT; or take into account the volume or value of referrals.

We believe that enactment of this type of safeharbor will help spur adoption of electronic health records and provide immediate benefits to consumers in the form of improved quality of care and patient safety.

In conclusion, HLC believes that HIT legislation should especially focus on areas in which Congress and the President *must act* to remove barriers and facilitate successful implementation of HIT. Therefore, HIT legislation should accelerate the adoption of health information technology and interoperable electronic health records by ensuring uniform IT standards including privacy and security and providing exceptions to Stark and anti-kickback rules to allow hospitals, medical groups and others to share their expertise and investment in electronic health records with physician offices. HLC will continue to work with Congress to continue to explore other funding mechanisms to promote wide spread adoption of HIT.

The Healthcare Leadership Council appreciates the opportunity to testify on the development of health care information technology, and I will also be pleased to discuss in greater detail with the subcommittee our firsthand experiences with health information technology at Evanston Northwestern Healthcare. Any questions about my testimony or these issues can be addressed to me or to Ms. Theresa Doyle, Senior Vice President for Policy, Healthcare Leadership Council (telephone 202-452-8700, e-mail tdoyle@hlc.org).

ATTACHMENT 1

Healthcare Leadership Council

Chief Executive Task Force on Quality and Patient Safety
Technical Advisory Board on Health Information Technology

Recommendations to Congress to Advance Implementation of Health Information Technology

June 2004 - Update

Acknowledgements

Many organizations, individuals, and institutions graciously provided input to this effort. Without their insight, time, and expertise, the effort would not have been successful. We would like to extend our special thanks to the Healthcare Leadership Council Technical Advisory Board and the individual participants (listed below) who provided the information that made this report possible.

Ascension Health	**Sherry Browne**, Chief Information Officer
Baylor Health Care System	**Robert Pickton**, Senior Vice President, Chief Information Officer, Baylor Information Systems
CIGNA Corporation	**Paul Oates**, Business Systems Architect
Evanston Northwestern Healthcare	**Thomas Smith**, Chief Information Officer
	Dr. Ned (Arnold) Wagner, Jr., Associate Professor, Chair, Medical Informatics Committee
Guidant Corporation	**William McConnell**, Vice President, Chief Information Officer
Mayo Clinic, Rochester	**Walt Menning,** Administrator, Information Services
	Bijoy Khandheria, MD, Chair, Information Management and Technology Committee
Mayo Clinic, Jacksonville	**John Mentel, MD,** Chair, Department of Applied Informatics
New York Presbyterian Hospital	**Edward (Ted) Shortliffe, MD, PhD,** Professor and Chair, Department Biomedical Informatics, Deputy Vice President for Information Technology, Health Sciences Division, Columbia University
	Gil Kuperman, MD, PhD, Director, Quality Informatics
Pfizer, Inc.	**Ross Martin, MD, MHA,** Senior Manager, Strategic Technology Group
	Dr. Steven E. Labkoff, MD, FACP, Director, Strategic Technology Group
Premier, Inc.	**Larry Grandia**, Membership Leadership Team
Vanderbilt Medical School	**Dr. Bill Stead**, Head of Informatics
Vanderbilt University Medical Center	**Nancy M. Lorenzi, PhD**, Professor of Biomedical Informatics, Assistant Vice Chancellor for Health Affairs
VHA, Inc.	**Michael Cummins**, Senior Vice President, Chief Information Officer

CONTENTS

Acknowledgements i

EXECUTIVE SUMMARY iii

Key Findings and Themes iii
HIT Benefits iii
HIT Barriers v
Recommendations v

Introduction and Background 1

Methodology 1

Key Findings and Themes 2

I. Members' HIT Applications 2
Clinical Applications of HIT 2
Table: Clinical Uses of HIT 3
Administrative Applications of HIT 4

II. HIT Benefits 4
Table: Summary of Cited HIT Benefits 6

III. Measuring Return on Investment 7

IV. HIT Challenges and Barriers 8
HIT Costs 8
HIT System Implementation Issues 9
Inadequate Standards and Lack of Interoperability 9

V. HLC Members' Successful HIT Implementations: Key Factors 10
Organizational Culture and "Buy-In" 10
Staffing and Training 11
Organizational Expectations 12
Organizational Business Processes 12

Recommendations 12

Conclusions 17

Appendix A: Discussion Questions to Guide HLC Conference Call on Health Care IT A-1

Appendix B: Selected References and Resources B-1

EXECUTIVE SUMMARY

The Healthcare Leadership Council (HLC) has a long-standing commitment to improved quality of care and patient safety. HLC envisions a 21st century health care system that is integrated and linked by information technology, that is consumer-centered, and that utilizes new drugs, technologies, and medical procedures to perform the highest quality health care. Achieving this vision is dependent upon health care delivery that is effective and cost efficient. For this reason, HLC has maintained a strong interest in facilitating health information technology (HIT) and supports its accelerated adoption and deployment.

HLC members have a unique understanding and successful history in implementing HIT. In summer 2003, HLC established a Technical Advisory Board comprised of clinicians and others with information technology expertise within HLC's member companies to provide information about their HIT implementation experiences. In total, 17 teleconferences were conducted with individuals representing multiple perspectives, including providers, managed care organizations, payers, pharmaceutical companies, and health care delivery systems.

This report summarizes the views and observations of participants in those teleconferences. No comments are attributed to individuals or to organizations.

Key Findings and Themes

Health information technology solutions have long been and continue to be offered as a key factor in improving health care quality and efficiency. HIT has been around for decades, but the industry is still a long way from achieving full implementation. It is becoming increasingly apparent, however, that investments in HIT provide significant returns across a variety of metrics. ***HIT provides increased delivery system efficiencies and cost savings, contributes to greater patient safety and better patient care, and achieves clinical and business process improvements.*** Patients benefit from the comprehensive adoption of HIT and the ability to share data within and across sites of care and among clinicians. Ultimately, other stakeholders such as employers, payers, policy makers, public health officials, and regulators will benefit from the ability to share and exchange data. In short, the return on investment in HIT is significant for all parties involved.

HIT Benefits

Several HLC member organizations were among the earliest adopters and pioneers of HIT. For HLC members, specific benefits (and lessons learned) typically vary by several factors, such as delivery system, organization or entity, data network, and organizational culture and staff mix (i.e., on-staff or employed physicians versus community-based physicians).

Healthcare Leadership Council
June 2004 – Update

HLC members have and continue to implement a wide range of clinical, financial and administrative applications and use diverse methods to develop systems. The following table summarizes the diverse benefits of HIT.

CLINICAL	ADMINISTRATIVE AND ORGANIZATIONAL	FINANCIAL
Reduced medication and other medical errors	Increased staff productivity	More accurate capture of codes and charges
Fewer and avoided adverse events	Increased access to data	Fewer rejected claims
Better communication between patients and clinicians	Increased job satisfaction	More efficient recruitment of qualified clinicians
Better communication with referring physicians	Enhanced recruitment of qualified nurses and other clinicians	Fewer duplicative tests
More timely and comprehensive infection control processes	Easier and more efficient data collection	Decreased operating costs
Increased time for hands-on patient care	Improved work flow	Reduced storage and transcription costs
Improved patient confidence in care	More efficient data flow to payers	Reduced per claim processing costs
Better information for clinical decisions and treatment options	More accurate, legible, and timely clinical documentation	Reduced supply costs
Fewer inpatient hospitalizations	Better compliance with regulatory requirements	
Reduced practice variation	Significant skill enhancement for nurses	
Improved patient satisfaction	Less redundant data entry	
Decreased patient waiting times	More timely public health reporting	
Better patient compliance with treatment plans	Improved data quality for research and clinical trials	
Streamlined disease and case management	Streamlined administrative processes	
	Improved data capture for use in national quality of care, clinical outcomes, and benchmarking efforts	
	Enhanced physician recruiting via EHR	

HIT Barriers

HLC participants highlighted a number of significant barriers, among them costs, standards, and interoperability. For example, in their quest to improve the quality of patient care, many health care providers, payers, and manufacturers continue to take advantage of information and communications technology. Unfortunately, their growing difficulty in investing scarce resources into increasingly expensive HIT, as well as the current lack of standards for HIT systems, have hampered the widespread adoption and implementation of these technologies.

Several participants cited an important yet often overlooked that must be taken into account reality regarding the costs and benefits of HIT systems. Providers that invest in or implement HIT absorb the full cost of system acquisition and implementation, but the benefits accrue to many others, including insurers, benefit managers, employers, regulators, patients, and the community as a whole.

Recommendations

In order to accomplish the widespread adoption of HIT, the Healthcare Leadership Council calls on the federal government to provide leadership, direction, and the capital necessary to spur the rate of diffusion through the entire health care system. Based on its members' successful track record, research, and "real world" experience, HLC offers the following recommendations, which can be organized into three broad categories:

- Standards to assure interoperability.
- Financial incentives and funding mechanisms.
- Liability protections to facilitate sharing of safety and quality data.
- Stakeholder collaboration on best practices.

***Recommendation 1.* The federal government should continue to oversee a comprehensive program of health data and information standards development that will facilitate exchange and sharing of data and information.**

Such standards will foster smooth and efficient communications and cooperation, regardless of individual system structure or architecture. Among other things, this work should address the increasing need for data, connectivity, interface, and communications standards. The health care industry also needs standards for commonly accepted clinical definitions, vocabulary, and terminology. Finally, this effort must also address concerns about patient privacy and confidentiality.

***Recommendation 2.* The federal government should implement financing mechanisms to spur private-sector HIT investment and accelerate the widespread adoption of HIT.**

This is designed to ease the financing crisis facing those attempting to adopt and implement often high-cost, highly complex HIT. Such financing mechanisms could

include: payment "rewards" or "add-ons", creation of an HIT revolving loan fund to invest public dollars in HIT projects and programs (e.g., modeled after the "Hill Burton" program); a revolving loan fund with debt forgiveness in accordance with specified criteria such as savings to the Medicare trust fund, tax incentives, reimbursement incentives based on improved patient outcomes, and matching private funds with public funds through grants from the Departments of Health and Human Services and the Department of Homeland Security.

Recommendation 3. ***Congress and the Administration should pass legislation to encourage open sharing of patient safety data by providing liability protections for certain disclosures of such data.***

A voluntary reporting system with strong legal protections for patient safety data is critical for improving the safety of the health care system. An environment where providers can share information for purposes of patient safety without fear of being sued will promote open disclosures of information about adverse events to designated patient safety organizations. Analysis of such disclosures can lead to system safety improvements. Legislation to accomplish this has been considered (but not passed) by Congress for the past three years. This legislation strikes a fair balance between protecting disclosures for patient safety purposes, while still protecting patient's legal rights by permitting use and disclosure of information that exists separately from the patient safety data. Electronic exchange and interoperability of health care information systems plays a critical role in an error reporting system described above.

Recommendation 4. ***Stakeholders should collaborate in the dissemination of best practices and lessons learned to further the successful implementation of HIT systems with proven functionality.***

HLC supports both industry-initiated and federally led dissemination of information about HIT implementation, including best practices and lessons learned. Such dissemination would allow and encourage additional collaboration among stakeholders, facilitate knowledge and experience sharing, and ultimately help providers and organizations utilize HIT to improve patient safety and quality of care.

A federal investment in private sector HIT will go a long way toward improving the quality, safety, cost, and effectiveness of health care.

Healthcare Leadership Council
June 2004 – Update

Introduction and Background

The Healthcare Leadership Council (HLC) has a long-standing commitment to improved quality of care and patient safety. HLC envisions a 21st century health care system that is integrated and linked by information technology, that is consumer-centered, and that utilizes new drugs, technologies, and medical procedures to perform the highest quality health care. Achieving this vision is dependent upon health care delivery that is efficient and cost effective. For this reason, HLC has maintained a strong interest in facilitating health information technology (HIT) and supports its accelerated adoption and deployment.

HLC members have a unique understanding and successful history in implementing HIT. Several HLC member organizations were among the earliest adopters and pioneers of HIT. Some are involved in the National Library of Medicine's (NLM) program providing grant support to health-related institutions and organizations for projects to plan, design, test, and deploy systems and techniques for integrating data, information, and knowledge resources into a comprehensive networked information management system.[1] Additionally, some participated in various Institute of Medicine (IOM), General Accounting Office (GAO), and Agency for Healthcare Research and Quality (AHRQ) studies and committees. Others are actively involved in national standards-setting organizations and related projects (i.e., Health Level 7 (HL7)).

After examining members' in-depth and diverse hands-on experience in HIT research and implementation, this paper discusses the many applications of HIT, the challenges and benefits of implementing HIT, and some key factors for successful implementation of HIT. We also offer three recommendations for furthering the adoption of HIT.

Methodology

In summer 2003, HLC established a Technical Advisory Board comprised of clinicians and others with information technology expertise within HLC's member companies to provide information about their HIT implementation experiences. In total, 17 teleconferences were conducted with individuals representing multiple perspectives, including providers, managed care organizations, payers, pharmaceutical companies, and health care delivery systems.

This report summarizes the views and observations of participants in those teleconferences. No comments are attributed to individuals or to organizations.

[1] NLM has supported such efforts to build integrated advanced information management systems (IAIMS). IAIMS are computer networks that link and relate the published biomedical knowledge base with individual and institutional databases and information files, within and external to an institution.

Key Findings and Themes

Participants shared their success stories and expressed diverse viewpoints reflecting their far-reaching experiences with HIT implementation. HLC members have implemented and continue to implement a wide range of clinical, financial, and administrative applications and use diverse methods to develop systems. Participants uniformly noted that the ability to exchange accurate information quickly within and across systems is essential in order to achieve a positive impact on health care delivery and related services. This section summarizes the major themes and participant recommendations.

I. Members' HIT Applications

Clinical Applications of HIT. HLC members—providers, pharmaceutical companies, medical device manufacturers, payers, and group purchasing organizations—are very involved in HIT projects and described various successful applications and IT-enabled processes across the entire continuum of health care. While clinical applications of IT, such as electronic prescribing, electronic health records (EHR), and digital imaging are most pervasively used in hospital settings, it is notable that a broad spectrum of health care industry sectors plays a role in clinical HIT applications that, combined, have great potential to increase the quality and safety of the health care system.

For example, several HLC pharmaceutical manufacturer members have been instrumental in facilitating patient bedside bar code verification during drug administration by voluntarily producing unit dose packages printed with standardized bar codes. Some pharmaceutical companies have developed on-line disease management programs using sophisticated data systems. Insurers also have implemented on-line disease management programs using automatic alerts for both patients and clinicians. And one insurer participant discussed the company's sophisticated claims data mining system that helps classify providers according to the quality of care they provide. The insurer makes this information available on line to help its enrollee's select high-quality providers.

Hospital group purchasing organization participants discussed their innovative programs to collect data from their hospital members and use it to perform benchmarking to help develop and disperse best practices for diabetes and other diseases. This data is also being used in a demonstration project to reward providers for providing a higher level of care quality. Comments were made during this particular discussion that standardized clinical nomenclature would greatly improve the value of this quality improvement tool.

A medical device manufacturer participant described one of the latest clinical applications of HIT that allows human implanted medical devices automatically to report health data to an online electronic health record. The success of this technology is, of course, dependent upon widespread use of electronic health records.

The table below summarizes clinical uses of HIT and the types of organizations most likely to use these applications.

Clinical Uses of HIT

	Hospital Inpatient	*Hospital Out-patient*	*Office Practice*	*Insurer /MCO*	*Medical Device Manuf.*	*Group Purchas. Org.*	*Pharma Manuf.*
Computerized physician order entry (CPOE)	✔	✔	✔				
Bedside bar coding	✔	✔					✔
Electronic health record (EHR)	✔	✔	✔				
Health record data mining	✔	✔		✔		✔	
Automated clinical guidelines and protocols	✔	✔	✔	✔		✔	✔
Digital imaging	✔	✔					
Provider and patient web-based communication	✔	✔	✔				
HEDIS data collection	✔	✔		✔		✔	
On-line disease management programs	✔	✔		✔		✔	✔
Prevention outreach	✔	✔		✔			
Data collection for assessing quality of care	✔	✔		✔	✔	✔	✔
Physician alerts	✔	✔	✔	✔			✔
Knowledge management applications	✔	✔		✔			
Patient reminders	✔	✔	✔	✔			✔
Decision support systems	✔	✔		✔		✔	✔
Clinical data warehousing	✔	✔		✔			
Assisting patients in provider selection	✔	✔		✔		✔	
Telemedicine	✔	✔					
Picture archiving and communications systems (PACs)	✔	✔					
Implanted medical device automatic data reporting and transmission to EHR	✔	✔	✔		✔		

Administrative Applications of HIT. In addition to the clinical application of information technology, participants discussed administrative applications such as patient registration, appointment scheduling, claims submission, eligibility verification, and billing. Comments were made that highly automated administrative systems linked with the organization's clinical systems not only free resources for more hands-on patient care, but also greatly increase patient and provider satisfaction as a result of less paperwork.

II. HIT Benefits

HLC member discussions revealed that HIT has had, and will continue to have, an enormously positive impact on health care practice and delivery within their organizations, enhancing patient safety and quality, and ultimately lowering costs. For HLC members, specific benefits (and lessons learned) typically vary by several factors, such as delivery system, type of organization or entity, data network, and organizational culture and staff mix (i.e., on-staff or employed physicians versus community-based physicians).

Increased patient safety is a highly desirable benefit of HIT systems, although a difficult benefit to quantify. However, one vendor participant noted that a university hospital system using bedside bar code technology has realized an 89 percent reduction in medication administration errors. The same university has realized an 85 percent improvement in documentation accuracy in the emergency room and 71 percent reduction in overall discrepancies utilizing an automated drug dispensing system.

In addition to increased quality of care and patient safety and reduced costs, ***increased satisfaction for patients and providers*** was overwhelmingly cited as a highly valued benefit of HIT systems. Satisfaction was often attributed to easier and quicker access to clinical information which decreases waiting times, repeat appointments and laboratory tests, paperwork, and redundant data collection for both clinicians and patients.

Well-functioning HIT systems contribute to ***increased satisfaction among physicians and nurses*** for other reasons as well, according to several participants. Increased enthusiasm for HIT systems was noticeable once clinicians were convinced that it was an important factor in better patient care. One organization that had implemented a computerized physician order entry (CPOE) system, for example, determined through internal surveys that physician satisfaction had noticeably increased in large part because the physicians believed patients were receiving better care as a result of the new system.

At a time of severe health care workforce shortages, HLC member organizations have found their HIT systems to be ***beneficial for recruiting and retaining health care workers***, especially nurses. Improving nurses' job satisfaction by transforming the way nurses practice nursing was raised frequently as a benefit of HIT. HIT has made tangible improvements in nurses' work processes such as infection control review and

case management. One hospital system participant with a very advanced HIT system said that, before implementing its electronic health record (EHR) system, nurses spent 30 percent of their time "hunting and gathering" scattered patient information; with the EHR system, time spent collecting data has been reduced to a fraction of the previous amount. Participants also cited HIT systems as valuable attractions for recruiting younger nursing graduates who see information technology as an integral part of their skill development as nursing professionals.

Collecting accurate data more efficiently to help consumers make better choices about their care was also frequently noted as an important HIT benefit for HLC's member organizations. Electronic data used in EHRs, electronic prescribing systems, digital imaging, or other HIT applications facilitate the assemby of more complete and accurate data across multiple sources. This contributes to better case and disease management, more accurate treatment options, and the ability to direct patients to higher quality and lower cost care.

In addition, HIT applications that combine administrative, financial, and clinical information systems benefit health care organizations, participants said, by allowing more accurate, timely, and complete data for data mining, predictive modeling, and financial analyses.

The following table summarizes benefits of HIT cited during our interviews:

Summary of Cited HIT Benefits

CLINICAL	ADMINISTRATIVE AND ORGANIZATIONAL	FINANCIAL
Reduced medication and other medical errors	Increased staff productivity	More accurate capture of codes and charges
Fewer and avoided adverse events	Increased access to data	Fewer rejected claims
Better communication between patients and clinicians	Increased job satisfaction	More efficient recruitment of qualified clinicians
Better communication with referring physicians	Enhanced recruitment of qualified nurses and other clinicians	Fewer duplicative tests
More timely and comprehensive infection control processes	Easier and more efficient data collection	Decreased operating costs
Increased time for hands-on patient care	Improved work flow	Reduced storage and transcription costs
Improved patient confidence in care	More efficient data flow to payers	Reduced per claim processing costs
Better information for clinical decisions and treatment options	More accurate, legible, and timely clinical documentation	Reduced supply costs
Fewer inpatient hospitalizations	Better compliance with regulatory requirements	
Reduced practice variation	Significant skill enhancement for nurses	
Improved patient satisfaction	Less redundant data entry	
Decreased patient waiting times	More timely public health reporting	
Better patient compliance with treatment plans	Improved data quality for research and clinical trials	
Streamlined disease and case management	Streamlined administrative processes	
	Improved data capture for use in national quality of care, clinical outcomes, and benchmarking efforts	
	Enhanced physician recruiting via EHR	

III. Measuring Return on Investment

Discussions among the HLC participants and examples of quantifiable benefits from their institutions indicate that methods to measure HIT benefits vary widely, although measures generally include both formal and informal analyses of financial impacts.

Some institutions use a return on investment (ROI) methodology to assess the financial impact of service-related operating expenses compared to revenue gains from improved service delivery. In some instances, the measurable financial improvements attributed to or facilitated by an information system have included the ability to control or reduce operating expenses (such as those related to personnel, printing, transcribing or storage costs), or to expand the types and range of services offered by the health care organization. Several participants described measuring positive financial outcomes in terms of quantifiable improvements in operating expenses or as new revenue for their health systems.

To fully calculate quantifiable benefits or ROI measurements, participants reported that they ***first determine the baseline measures of specific metrics*** and then perform formal *projected* return on investment or cost benefit analyses before investing in HIT systems. Several organizations reported the difficulty of making such assessments, however, because of the long length of time HIT implementation often requires before the old system can be integrated or dismantled. For example, one hospital system began implementing HIT systems in 1991, and it was not until 1999 that they had enough infrastructure in place to be able to begin taking costs out of the combined old and new systems. In contrast, one system cited that, in just two months after getting its EHR system off the ground, it collected the same revenue with fewer patients, and after four months it was taking in more revenue with the same number of patients. Clearly, factors such as the size of an organization, the patient population, the intensity of the HIT application as well as many others make it difficult to compare costs versus benefits across sites.

Another participating organization pointed out that formal evaluations of returns on investment are seldom conducted because they are an expensive, added cost. This system felt confident that it was receiving a return, without the official analysis. It was noted that cost savings from personnel reductions and transcription costs were evidence that the organization was receiving financial returns, and that the increased ability to deliver better quality and safer health care overshadowed the need to prove a financial return.

Other HLC members also measured benefits in ***more qualitative and perhaps intangible terms***. For instance, participants indicated that benefits resulting from implementing patient access to personal health records, patient-physician electronic messaging, and automated appointment scheduling include better communication, less hassle, and improved patient satisfaction. Maintaining critical staff and enhancing continuity of patient care were also raised as "returns on investment." These and other benefits of HIT mentioned previously in this paper might be difficult to measure, but as

many participants pointed out, they intuitively translate into indirect cost savings for an organization.

There was general agreement that successful HIT implementation requires significant investments of time and therefore a system's financial return should also be measured over time because benefits are not always immediate.

IV. HIT Challenges and Barriers

Along with the benefits, HLC participants described several challenges in implementing HIT. One obvious challenge is that health care is fragmented and delivered by various providers across multiple settings. Clinical information is complex and there are logistical difficulties in information sharing across settings. Additionally, clinicians need access to larger amounts and increasingly more complicated kinds of information in order to provide adequate care. Health care organizations themselves are complex, presenting added challenges for information sharing. Legislative and regulatory requirements governing patient privacy and confidentiality add yet another layer of challenge. Finally, the health care industry continues to face increasingly technical and dynamic regulatory pressures and requirements.

HLC participants highlighted a number of other significant barriers, among them costs, standards, and interoperability.

HIT Costs. A lack of funding or adequate resources—combined with the high costs of HIT systems—was repeatedly cited as a barrier to effective implementation of HIT systems. There are ***significant front-end and ongoing maintenance and operational costs*** for HIT, including software, hardware, training, upgrades, and maintenance. Systems and products are virtually unaffordable for those providers who do not have ready access to the needed operating capital. In addition, health care organizations often view systems implementation as very time-consuming, which translates into another layer of costs.

Transitioning from existing paper-based or long-standing IT legacy systems is an expensive proposition. Systems that were implemented in earlier decades, many of which still exist, were often installed as stand-alone systems. Costs to replace or to integrate these systems are significant, as are costs for ongoing systems maintenance and upkeep.

In addition to capital costs, ***ongoing operational costs*** in any institution require careful consideration. One participant noted that health care providers typically commit to increased spending of about 3 percent for operational costs when planning IT projects. Other information-intensive industries–banking, insurance, investment houses–commit more than double or triple that number for operating IT systems. This participant believes that an EHR system requires at least a 4 or 5 percent increase in spending for ongoing operational costs.

Several participants cited an important yet often overlooked reality regarding the costs and benefits of HIT systems that must be taken into account. Providers that invest in or implement HIT ***absorb the full cost of system acquisition and implementation***, but the benefits accrue to many others, including insurers, benefit managers, employers, regulators, patients, and the community as a whole.

Given these challenges, there are concerns that the pace and pattern of HIT adoption will not be uniform and will be too prolonged to have a significant impact on quality and safety in the foreseeable future.

HIT System Implementation Issues. Some participants discussed the difficulties of finding the "right" systems solutions among many HIT systems options. Major hospital system mergers have presented the challenge of integrating multi-vendor systems that have historically been incompatible. One participant described how his organization had to consolidate more than 70 products from 35 vendors across hundreds of provider sites to create a comprehensive HIT infrastructure leveraging the organization's existing investments and legacy systems.

Regardless of mergers, as mentioned above, many HIT systems have been implemented over an extended period of time, beginning before the availability of many of today's commercial vendor products. These homegrown legacy systems must frequently be factored into the design of an organization's new HIT infrastructure; however, incorporating them into a new system design usually requires costly trade-offs in terms of speed of implementation and the ability to share data between organizations. Consolidation of multiple vendor products and legacy systems can be extremely challenging and costly. Developing tailored or customized systems in conjunction with vendors and implementing various commercial off-the-shelf (COTS) vendor products are among the daunting array of choices for HIT systems that organizations must investigate when trying to implement or integrate an HIT system.

Several participants were encouraged by a very recent evolution taking place among HIT vendors that seems to be resulting in more versatile HIT systems with greater user satisfaction and interoperability. This may be largely a result of vendors working more closely with their customers to develop commercial systems. One teaching institution participant, for example, worked over a period of several years with a major HIT vendor to develop a commercial CPOE system that was fine tuned through years of physician trial and feedback about content and usability.

One participant of a very large hospital system stated that she did not perceive a lack of quality HIT products and vendors, but is instead challenged by the short supply of knowledgeable, high-quality IT personnel to maintain HIT systems in the long term.

Inadequate Standards and Lack of Interoperability. To achieve system-wide health care benefits of HIT, there is an increasing need for data, connectivity, interface, and communications standards allowing the sharing of data nationwide. For example, the EHR, as envisioned by many, implies total consolidation of all patient data from before

birth through death, accessible by those who need to know, and available at all points of care. This will require full interoperability within and across all health care settings. Additionally, uniform interoperability would eliminate the issues many health care systems now face as a result of mergers of several smaller systems.

While participants acknowledged the importance of this "next step" of macro-interoperability, most are moving forward with implementation of HIT systems even in the absence of standards that would allow their systems to interface with other health organizations nationwide. There are still standards, however, that some stated as being necessary to help their individual HIT systems function better. One standard that was repeatedly cited as necessary to improve internal systems was ***a commonly accepted clinical vocabulary***. Lack of such a standard has contributed to costly, cumbersome, and inefficient retrospective data mining. Hope was expressed by several participants that the Department of Health and Human Services' recent action to publicly license SNOMED—a comprehensive set of clinical reference terminology that the health industry can use to improve the comparability of data—would prove an important step to resolving this particular problem.

Contributing to the interoperability challenge is the fact that health care is complex and no two providers, settings, or institutions are identical. ***A successful solution in one setting is not necessarily transferable to another.*** As discussed previously, in many instances, providers have merged into or have formed larger (integrated) delivery systems often resulting in numerous disparate and sometimes duplicative systems. In some cases we learned that even existing systems within organizations cannot communicate with each other.

All of these issues contribute to a fragmented use of technology with minimal interoperability. Federally driven standards (with appropriate testing and implementation considerations) could potentially go a long way toward resolving technical and technological constraints due to variations (and incompatibilities) among system configurations, architectures, and platforms.

V. HLC Members' Successful HIT Implementations: Key Factors

Participants provided keen insight into successful HIT implementations based on their firsthand knowledge and long-standing experiences. They described several key factors influencing HIT implementations, including organizational culture, access to capital, and long-term commitments in terms of time and people.

Organizational Culture and "Buy-In". An organization with a pervasive philosophy of continuous quality improvement and error reduction is bound to be more successful at HIT implementation. This foundation is laid through strong dedication and involvement of top executive leadership in process innovation and improvement well before commencing HIT systems implementation. Conversely, several participants stated the underlying danger of implementing expensive HIT systems on top of existing inefficient and poorly managed disparate processes.

Detailed preparation and involvement of clinical, technical, and other staff were also mentioned by many participants as being necessary factors in HIT systems success. Anticipating and overcoming staff resistance or unwillingness to use the HIT system were critical.

Making sure that clinicians are proponents of the system was raised by all participants. ***It is essential, they said, that clinicians, especially physicians and nurses, actively participate in and support the development and implementation of any HIT solution from the very early stages.*** Several examples for gaining clinician "buy-in" for HIT implementation were cited. These included using team processes and staff-driven decision-making criteria and ensuring that computer technicians and clinicians engage in ongoing dialogues throughout design and implementation. Not only does this involvement help increase acceptance among clinicians, it also allows for incorporation of specific features and functions specifically designed to support the clinicians' unique work processes and needs.

One organization, for example, used a team of physicians to help design its EHR. The participant from that organization described the organization's willingness to compromise between an "engineering marvel" and a system that was acceptable and would be usable by the organization's physician staff.

The extent to which the use of HIT systems is "mandated" versus voluntary for clinicians (especially attending physicians) varied with the specific type of organization and HIT application. One hospital system definitively mandates that if physicians want to work in that hospital system, they must use the hospital's EHR. Another participant reported that, while the use of its EHR system was voluntary, more than 70 percent of clinicians were doing direct data entry using the automated systems. Interestingly, in cases where using the hospital's HIT systems is voluntary, there was little variance in physician user acceptance between staff models where the physicians are employees of the hospital versus models where the physicians are independent practitioners at the hospital.

Several participants said a key factor in influencing an "HIT culture" is to provide evidence to clinicians of improvement in safety and quality of care. One example offered involved improved outcomes data from fetal monitoring. In this case, there was enough evidence of improvement to compel an immediate practice change, which no physician resisted once shown the data. Similar results were demonstrated with nursing personnel. One respondent discussed the greatly increased level of commitment to IT by nurses who were presented with case studies of increased safety that resulted from automated systems.

Staffing and Training. The importance of up-front and ongoing staff training cannot be overstated, according to the participants. It is critical to make certain that staff is well trained and proficient in its use of HIT in order to assure acceptance and adoption of the system. One participant mentioned that each physician is required to complete 16 hours of electronic health record training in order to work at the hospital, in many cases required training hours exceeding that. Other participants remarked that taking the

system and the training to the clinicians on the floors and at the bedside—not in the classroom—was also critical.

Organizational Expectations. Repeatedly, participants stressed the need to establish clear expectations of HIT implementation projects. Organizations implementing HIT systems need to identify expected accomplishments and benefits and link what will be invested with what will be achieved. Expectations can include better communication between patients and clinicians, increased job satisfaction among clinicians, improved workflow, more efficient data sharing and communication, lower operating costs, and better information to make clinical decisions.

One participant stated the importance of recognizing differences across organizations in terms of cultures, patient bases, environments, attitudes, priorities, size, complexity, and scope of services provided. This means that a successful system in one location will not necessarily meet the requirements or expectations at another.

Another important point made was that institutions must recognize that HIT systems implementation is an ongoing evolutionary process. HLC members noted that their personal and organizational involvement in specific systems implementation often spanned decades. One participant described her health system's HIT plan in particularly far-sighted terms. The health system, which was once three smaller systems, is focused on trying to ensure that each hospital has a minimum foundation of IT integration that can eventually lead to CPOE, digital imaging, and an electronic health record. Just installing this minimal foundation, however, is expected to take several years.

Organizational Business Processes. Success depends, in part, upon factors related to how the institution conducts its business plan for HIT implementation, according to the participants. This includes methods of management and project design, selected aspects of service redesign and consolidation, integration of services across sites, and their effects on staff and productivity. Related to this is the need to coordinate HIT planning and investment management techniques across the enterprise. Consolidating common HIT functions, processes, and applications are also critical to successful implementation.

Recommendations

Based on its members' successful track record, research, and "real world" experience, HLC offers the following recommendations, which can be organized into four broad categories:

- Standards to assure interoperability.
- Financial incentives and funding mechanisms
- Liability protections to facilitate sharing of safety and quality data.
- Stakeholder collaboration on best practices.

Recommendation 1. ***The federal government should continue to oversee a comprehensive program of health data and information standards development that will facilitate exchange and sharing of data and information.***

The federal government, working with private industry, should continue to establish agreement on basic rules for open, nonproprietary, and scalable system connectivity rules, operating protocols, data definitions, and data element specifications. The government should strongly encourage the use of these standards so that the same (versions of) standards are implemented and updated simultaneously across the industry. In order to overcome the continued lack of interoperability, HIT vendors need to implement systems in accordance with universally accepted standards so that different systems will work with each other. Obviously, such standards must address concerns about patient privacy and confidentiality.

The Department of Health and Human Services (HHS) is already playing a leadership role in fostering the development of data standards and encouraging investments to identify and speed the adoption of new technologies throughout the health care system. HHS efforts to date include the Consolidated Health Informatics Initiative (CHI) and support for the National Health Information Infrastructure (NHII). Both activities have contributed to the adoption of standards for federal health programs. There are many public-private activities underway to build the NHII, an idea noted in an Institute of Medicine (IOM) report on computer-based patient records in 1991 and then elaborated upon in a 2001 National Committee on Vital and Health Statistics Report.[2] The concept has since been endorsed by a variety of public and private sector organizations. The broad goal of the NHII is to deliver reliable data in a secure and private format to patients, clinicians, and providers when and where they need it, so they can use this information to make informed decisions about health and health care services.

In July 2003, HHS asked the IOM and Health Level 7 (HL7),[3] to design a functional model and standard for the electronic health record; their efforts are ongoing.[4] In July 2003, HHS also announced that the department had signed an agreement with the College of American Pathologists to license the college's standardized medical vocabulary system and make it available without charge throughout the United States.

---

[2] National Committee on Vital and Health Statistics. "Information for Health: A Strategy for Building the National Health Information Infrastructure." Washington, D.C. November 15, 2001.

[3] HL7 is an accredited ANSI standard organization that produces the HL7 messaging standard. It is the accepted *messaging standard* for communicating clinical data. It is supported by every major medical informatics system vendor in the US. The HL7 mission is to provide a comprehensive framework and related standards for the exchange, integration, sharing, and retrieval of electronic health information that supports clinical practice and the management, delivery, and evaluation of health services.

[4] CHI is a collaborative effort between the Department of Health and Human Services, the Veterans Affairs/Veterans Health Administration, the Department of Defense, and other federal agencies to adopt government-wide health information standards. The first set of CHI standards were announced on March 21, 2003 and include: Health Level 7 (HL7) messaging standards; Logical Observation Identifier Name Codes (LOINC) to standardize the electronic exchange of clinical laboratory results; National Council on Prescription Drug Programs (NCDCP) standards for retail pharmacy transactions; Institute of Electrical and Electronics Engineers 1073 (IEEE1073) standards that allow for health care providers to plug medical devices into information and computer systems; Digital Imaging Communications in Medicine (DICOM) standards that enable retrieval and transfer of images and associated diagnostic information.

In April 2003, the Food and Drug Administration issued a proposed rule requiring the use of standardized bar codes on all levels of drug packaging, including unit-of-use packages.

While these are impressive efforts toward developing nationwide standards for HIT, a coordinated and accelerated initiative must take place to ensure that these and other standards and their related technologies are available for mainstream use in the near future.

***Recommendation 2.* Congress and the Departments of Health and Human Services and Homeland Security should implement financing mechanisms to spur private-sector HIT investment and accelerate the widespread adoption of HIT.**

The federal government should drive the nation's implementation of HIT by offering federally supported financing for capital and operations costs to help providers defray the huge costs of acquiring and operating HIT. The Department of Health and Human Services (HHS) should accelerate the development and disbursement of these financial incentives in order to encourage widespread HIT adoption. How soon the government ultimately supports such financing will be critical to the ultimate levels and patterns of HIT adoption across all segments of the industry.

Discussions revealed that, in the absence of federal financing mechanisms, it would be years before most providers adopt HIT. Generally, few believe that natural market conditions or private sector market competition will be enough to propel the needed level and pace of HIT adoption. On the other hand, incentives related to HIT implementation and operation would have a far-reaching and positive impact on the entire health care community, ranging from large enterprises to individual practices. Benefits of greater efficiency, productivity, and quality would diffuse to individuals and institutions throughout the health care system.

Rapid implementation of interoperable HIT is also considered a critical component of the nation's emergency preparedness. In a May, 2003, report, the General Accounting Office (GAO) states "Many of the activities underway to prepare for and respond to public health emergencies–including bioterrorism–are supported by information technology, which can better enable public health agencies to identify naturally occurring or intentionally caused disease outbreaks and can support communications related to public health." The report also states that "automated medical information systems can play an important role for clinicians during their response to a medical emergency, in documenting the treatment of illness and its outcome, and in collecting and sharing diagnostic test results." Additionally the report states, "The use of electronic medical records could reduce the burdensome and costly use of paper-based processes, facilitating rapid access to data critical for near real-time public health surveillance."[5]

[5] *Bioterrorism: Information Technology Strategy Could Strengthen Federal Agencies' Abilities to Respond to Public Health Emergencies*, General Accounting Office (GAO), May, 2003, GAO-03-139.

HLC advocates the consideration and implementation of multiple HIT funding mechanisms. Regardless of the option or options chosen, participants noted that the federal government should assume a leadership role and create a financial catalyst for widespread HIT adoption, particularly among providers. As mentioned previously, the beneficiaries of IT-driven quality and safety improvements extend far beyond the providers—a strong argument for public funding. Instituting new or expanded funding mechanisms to reward those who successfully implement HIT—to include initial system installation as well as system upgrades or maintenance and operations costs—is one of the more compelling strategies to accomplish widespread adoption of HIT.

Potential financing models or options include:

- ***Payment "rewards" or "add-ons" based on HIT implementation and operating costs.*** This could include direct payments for using specific HIT applications (such as CPOE), offering higher payments to providers who use HIT, or offering discounts on medical liability insurance for HIT implementers.

- ***A loan program with debt forgiveness in accordance with specified criteria***, such as demonstrating a savings to the Medicare trust fund by achieving specific patient safety or quality of care improvements.

- ***Creation of a HIT revolving loan fund to invest public dollars in HIT projects and programs.*** For instance, as some have proposed, these could be administered through community-level nonprofit lending agencies.[6] This could be a self-perpetuating fund as borrowers repay their loans and could be modeled after the "Hill Burton" program.[7] It could also include funding formulas and federal conditions of participation.

- ***Direct grants to designated organizations and providers*** based on established criteria and needs.[8] In addition to ongoing grant programs from the Department of Health and Human Services, the **Department of Homeland Security** could consider a grant program for facilitating the implementation and interoperability of HIT that can aid in health care delivery during an act of bioterrorism or other public health emergency.

---

[6] Coye, Molly Joel, Bernstein, William S., "Perspective: Improving America's Health Care System by Investing In Information Technology", Health Affairs, Vol. 22/No.4.

[7] The Hill Burton program was created by Congress in 1946 to give hospitals and other health facilities money for construction and improvement in exchange for providing a reasonable volume of services to those unable to pay and for making services available for all persons residing in the facilities area.

[8] For example, the Agency for Healthcare Research and Quality recently announced the availability of research grants to assess the value derived from the adoption, diffusion, and utilization of health information technology (HIT) to improve patient safety and quality of care. The HHS Office for the Advancement of Telehealth recently granted a total of $3.74 million to 15 existing telehealth programs. The awardees support clinical telemedicine, distance learning, and patient education/disease management programs.

- ***Tax incentives*** to stimulate private sector (especially provider) investment in HIT.

- ***Reimbursement incentives*** based on demonstrating designated levels of improved patient care outcomes or other established criteria. This could include an investment program based on federally developed standards of performance and tied to provider compliance with such standards or their ability to demonstrate performance in accordance with the criteria.

- ***Adjustment of payment policies*** to recognize designated HIT applications as a reimbursable service.

- ***Initiatives to match private funds with public funds*** via a grant and/or revolving loan program.

Recommendation 3. ***Congress and the Administration should pass legislation to encourage open sharing of patient safety data by providing liability protections for certain disclosures of such data.***

A voluntary reporting system with strong legal protections for patient safety data is critical for improving the safety of the health care system. An environment where providers can share information for purposes of patient safety without fear of being sued will promote open disclosures of information about adverse events to designated patient safety organizations. Analysis of such disclosures can lead to system safety improvements. Legislation to accomplish this has been considered (but not passed) by Congress for the past three years. This legislation strikes a fair balance between protecting disclosures for patient safety purposes, while still protecting patient's legal rights by permitting use and disclosure of information that exists separately from the patient safety data. Electronic exchange and interoperability of health care information systems plays a critical role in an error reporting system described above.

Recommendation 4. ***Stakeholders should collaborate in the dissemination of best practices and lessons learned to further the successful implementation of HIT systems with proven functionality.***

Commencing an HIT implementation project requires a daunting amount of research to evaluate constantly evolving commercial off-the-shelf products versus other options appropriate for an institution's unique environment and desired applications. Further complicating implementation plans it that some or all of an institution's legacy systems must be taken into consideration in the overall design. In some cases, institutions may form relationships with vendors to help them develop a "semi-custom" and effective system solution. In these cases, the provider organization often provides the clinical and organizational expertise for product development. In any case, researching and designing such systems contribute to the already high cost of implementation. Of even greater concern is the potential to waste limited funding by choosing applications or systems that may not maximize potential for increased safety and quality, or by failing to

consider adequately possible long-term complications. Given the expertise gained by many premier health care institutions pioneering HIT implementation, an industry-initiated effort to share best practices could potentially speed the adoption of HIT throughout the health care industry.

HLC also supports federally led (sponsored) dissemination of information about HIT implementation, including best practices and lessons learned. Such dissemination would allow and encourage additional collaboration among stakeholders, facilitate knowledge and experience sharing, and ultimately help providers and organizations utilize HIT to improve patient safety and quality of care.

Conclusions

From this work, HLC arrives at two overarching conclusions. First, that HIT holds enormous potential, but second, that it remains stymied by challenges and barriers—and that full implementation is still far off. With regard to the opportunities presented by HIT, it is becoming increasingly apparent that HIT will provide savings, contribute to greater patient safety, enhance patient care, allow for increased delivery systems efficiencies, and achieve clinical and business process improvements. [9] [10] HIT can drive across-the-board positive changes and enhance value in care delivery. In particular, applications such as electronic health records, electronic prescribing, and bedside bar coding have been identified and promoted as necessary to facilitate a safer and more efficient health care system. Patients will benefit from the comprehensive adoption of HIT and the ability to share data within and across sites of care and among clinicians. Ultimately, other stakeholders such as employers, payers, and regulators will benefit from the ability to share and exchange data.

However, as this report points out, the reality is that there has been limited adoption and implementation of HIT. Ultimately, more widespread adoption of HIT will eliminate or diminish duplicative information gathering and will help assure delivery of health care based on timely, relevant, and complete information. The federal government should develop and implement a comprehensive HIT-financing program to meet the wide variety of providers' needs and to be responsive to many stakeholders.

In the absence of federal leadership and specific initiatives, HIT implementation will continue in a piecemeal and fragmented fashion. HHS should facilitiate ongoing collaboration between the public and private sectors to establish consensus enabling interoperability within and across health care organizations. A federal investment in private sector HIT will go a long way toward improving the quality, safety, cost, and efficiency of health care.

---

[9] General Accounting Office (GAO) Information Technology. Benefits Realized for Selected Health Care Functions. October 2003. GAO-04-224.

[10] Patient Safety: Achieving a New Standard for Care. Institute of Medicine of the National Academies, November, 2003.

Appendix A: Discussion Questions to Guide HLC Conference Call on Health Care IT

Please describe the clinical HIT (health information technology) systems or applications that you have implemented. For each, please note whether the system is "home grown" or a COTS product:

Admission/discharge/transfer
Computerized physician order entry (CPOE)
Bar coding
E-prescribing
Pharmacy/medication management
Other?
Patient registration
Electronic health record
Laboratory results
Clinical decision support

What were/are the compelling reasons to implement HIT systems? What were/are the benefits of implementing HIT systems?

What were/are the (strategic, tactical, operational, financial, cultural) challenges regarding HIT implementation?

What do you perceive as the most common barriers and obstacles to implementing HIT systems?

What were/are potential solutions to overcoming these barriers?

What strategies did you use/do you recommend to (successfully) implement HIT systems?

What role did/does HIT have regarding patient safety? Organizational productivity? Efficiency?

What role did/does organizational culture have in your implementation?

What do we need to do to help assure the continued future implementation/deployment of HIT systems?

How have you measured the success of your efforts?

Could you describe your techniques for conducting cost-benefit analyses of HIT implementations? For calculating your ROI (return on investment)?

Appendix B: Selected References and Resources

Agency for Healthcare Research and Quality, Rockville, Maryland Bioterrorism Preparedness and Response: Use of Information Technologies and Decision Support Systems. Summary, Evidence Report/Technology Assessment: Number 59, July 2002.

Agency for Healthcare Research and Quality (AHRQ) Rockville, Maryland, Healthcare Informatics Standards Activities of Selected Federal Agencies (A Compendium), November 1999, 50 pp. (AHCPR 00-R004).

Agency for Healthcare Research and Quality (AHRQ). Patient Safety Reporting Systems and Research in HHS. Fact Sheet. April 2001. Rockville, Maryland.

Agency for Healthcare Research and Quality (AHRQ) Rockville, Maryland, Summary Report: "Current Healthcare Informatics Standards Activities of Federal Agencies," November 1999.

Agency for Healthcare Research and Quality (AHRQ), Rockville, MD. *Expert Panel Meeting: Health Information Technology*. Meeting Summary. September 2003. http://www.ahrq.gov/data/hitmeet.htm.

Agency for Healthcare Research and Quality (AHRQ) Rockville, Maryland, Case Study Finds Computerized ICU Information System Care Can Significantly Reduce Time Spent by Nurses on Documentation. Press Release October 10, 2003.

Agency for Healthcare Research and Quality (AHRQ) Rockville, Maryland Research in Action Issue 6 June 2002. Medical Informatics for Better Patient Care.

Alliance of Community Health Plans Foundation, Promoting Prevention Through Information Technology." October 2003.

Amatayakul, Margret, MBA, RHIA, FHIMMS. "The Role of Health Information Managers in CPR Projects." American Health Information Management Association, Chicago, Illinois,1999.

Ball, Marion, Garets, David E., Handler, Thomas. "Leveraging IT to Improve Patient Safety". Yearbook of Medical Informatics of the International Medical Informatics Association. February 2003.

Bates, David W., Gawande, Atul A., "Improving Patient Safety with Information Technology." New England Journal of Medicine 348, pp.2526-2534.

Brailer, David J, M.D., PhD., Terasawa, Emil L., A.B., "Use and Adoption of Computer Based Patient Records." California Healthcare Foundation, October 2003.

Boland, Peter, White, Karen, Wieners, Walter, and Peabody, John. "A Boost to Service and Quality." Healthcare Informatics. October 2003.

Briggs, Bill, "CPOE Order from Chaos.". Health Data Management. pp.45-48. February 2003.

Butler-Close, K., Schriger, D.L., Baraff, L.J., et.al. "Heterogeneous effect of an emergency department expert charting system." Annals of Emergency Medicine 41(5), pp. 644-652. May 2003.

California Healthcare Foundation. "Digital Hospitals Move off the Drawing Board." October 2003.

California Healthcare Foundation, "A Primer on Physician Order Entry." September 2000.

Corn M., K. Rudzinski, M. Cahn "Bridging the Gap in Medical Informatics and Health Services Research: Workshop Results and Next Steps." Journal of the American Medical Informatics Association, 9(2):March/April 2002, 140-143. (AHRQ 02-R060).

Coye, Molly Joel, Bernstein, William S., "Perspective: Improving America's Health Care System by Investing In Information Technology." Health Affairs. Vol. 22/No.4.

Detmer, Don, M.D., "Bridging the National Health Information Infrastructure for Personal Health, Health Care Services, Public Health, and Research."

Electronic Journal of Information Systems Evaluation, 3(1); March 2000. "The Elusive Nature of Delivering Benefits from IT Investment."

Fitzmaurice J.M., Adams K., and Eisenberg, J. "Three Decades of Research on Computer Applications in Health Care: Medical Informatics Support at AHRQ", Journal of the American Medical Informatics Association, 9(2):March/April 2002, 144-160. (AHRQ 02-R059).

General Accounting Office (GAO), Information Technology. Benefits Realized for Selected Health Care Functions. October 2003. GAO-04-224.

General Accounting Office (GAO), Bioterrorism: Information Technology Strategy Could Strengthen Federal Agencies' Abilities to Respond to Public Health Emergencies. May, 2003. GAO-03-139.

Goldsmith, Jeff, Blumenthal, David, and Wes Rishel, "Federal Health Information Policy: A Case of Arrested Development," Health Affairs, July/August 2003.

Health Information Management Systems Society (HIMSS), Chicago Illinois. "Position Statement on the HIT Revolving Load Fund." August 2003.

Institute of Medicine Report, "Patient Safety: Achieving A New Standard of Care." November 2003.

Institute of Medicine Letter Report, Committee on Data Standards for Patient Safety, "Key Capabilities of an Electronic Health Record System," July, 2003.

Institute of Medicine Report Priority Areas for National Action: Transforming Health Care Quality. January 7, 2003.

Institute of Medicine Report Fostering Rapid Advances in Health Care: Learning from System Demonstrations. November 19, 2002.

Institute of Medicine Report The Future of the Public's Health in the 21st Century. November 11, 2002.

Institute of Medicine Report Who Will Keep the Public Healthy: Educating Public Health Professionals for the 21st Century. November 4, 2002.

Journal of Management Information Systems, 16(4).. Special Issue: Impacts of Information Technology Investment on Organizational Performance. Spring 2000.

Journal of Management Information Systems, 16(4), Information Technology Payoff in the Health-Care Industry: A Longitudinal Study. Spring 2000.

Labor HHS Subcommittee Hearings and Testimony. Dr. John Mentel, David Bernd, Dr. James Fries, Dave Hickman, Donald Hoover. June 11, 2003.

Massachusetts Technology Collaborative. Innovation Outlook Series. "Advanced Technologies to Lower Health Care Costs and Improve Quality." Fall 2003.

Mentel, John, M.D. "Testimony before the Senate Appropriations Committee Subcommittee on Labor, Health, and Human Services", June 11, 2003.

National Action Agenda for the National Health Information Infrastructure. Recommendations of the Financial Incentives Track. July 2003.

National Committee on Vital and Health Statistics. "Information for Health: A Strategy for Building the National Health Information Infrastructure." Washington, D.C. November 15, 2001.

National Electronic Disease Surveillance System Working Group: National Electronic Disease Surveillance System (NEDSS): A standards based approach to connect public health and clinical medicine. J. Public Health Management and Practice 2001.

Ortiz, E., Meyer G., Burstin, H. "The Role of Clinical Informatics in the Agency for Healthcare Research and Quality's Efforts to Improve Patient Safety". Proceedings of the AMIA Annual Fall Symposium 2001 Philadelphia: Hanley & Belfus, 2001, 508-512.

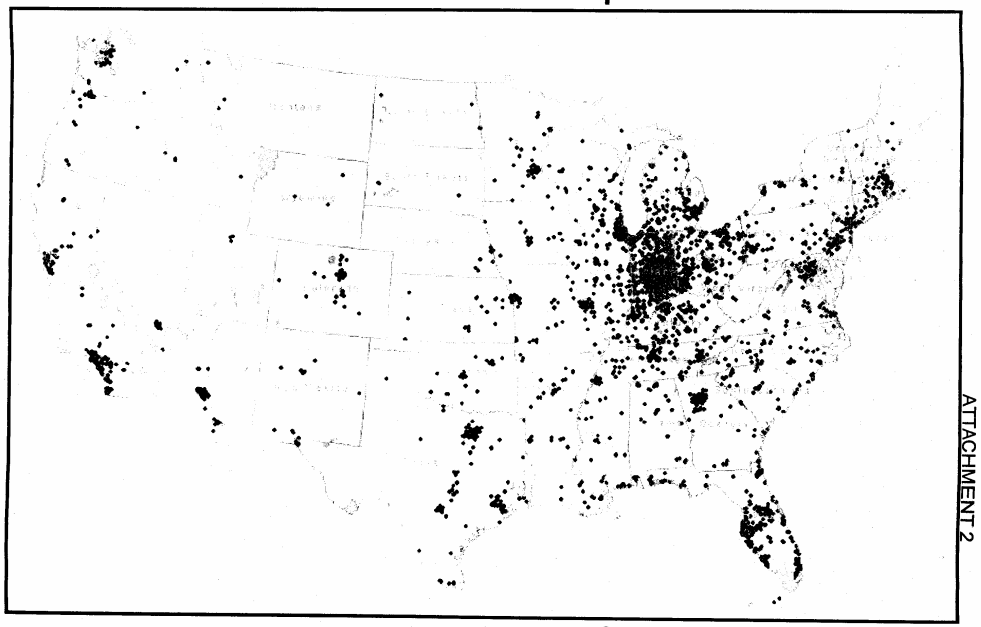
Ortiz, E., and Clancy, C.M. (2003 April)."Use of information technology to improve the quality of healthcare in the United States". Health Services Research 38 (2) pp.xi-xii.

Rosenstein AH "Measuring the Benefit of Performance Improvement and Decision Support." American Journal of Medical Quality.14(6):262-9. Nov-Dec 1999.

Rough, Steve, M.S. R.Ph., Director of Pharmacy, University of Wisconsin Hospital and Clinics. "Impact of Point of Care Bar Code Medication Scanning Technology." Presentation to the American College of Healthcare Executives. Boston MA. September 2003.

ATTACHMENT 2

Indiana Network for Patient Care
Home addresses of patients



Source: Indiana Network for Patient Care 2004

Attachment 3

November 16, 2005

The Honorable Nathan Deal
Chairman
House Energy and Commerce Subcommittee on Health
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

The undersigned organizations support the provisions within H.R. 4157, the "Health Information Technology Promotion Act of 2005," that would establish a process for achieving national uniform privacy and security standards for healthcare information based on the Health Insurance Portability and Accountability Act (HIPAA) regulations. Many of these organizations are members of the Confidentiality Coalition, a broad-based group of health and employer organizations founded to advance effective patient confidentiality protections.

We believe that efforts underway by Congress and the Administration to facilitate and encourage widespread adoption of interoperable electronic health records can greatly improve quality of care, reduce medical errors, and achieve greater efficiencies within our healthcare system. However, the lack of a national standard for patient privacy and security laws and regulations will impede these objectives. Without Congressional action, medical providers attempting to work together through interoperable health information technology systems would be subject to a confusing maze of state laws, rules, and regulations.

We believe these provisions offer an appropriate solution to this issue by allowing a state law study to be conducted first to determine the best way to achieve uniformity. If Congress fails to act upon the recommendations produced from the study, then HHS is charged with developing a uniform rule based on HIPAA. Importantly, these provisions provide a course of action and ensure that a national standard will be achieved.

Thank you for your leadership on this issue. We look forward to working with you and your staff on this important issue.

Sincerely,

Academy of Managed Care Pharmacy
Advanced Medical Technology Association (AdvaMed)
Aetna Inc.
American Benefits Council
American Clinical Laboratory Association
American Health Information Management Association
American Hospital Association
American Managed Behavioral Healthcare Association
American Medical Group Association
America's Health Insurance Plans

Amerinet
AmerisourceBergen Corporation
Ascension Health
Association of American Medical Colleges
Baxter Healthcare Corporation
Blue Cross and Blue Shield Association
Cardinal Health
CIGNA
The ERISA Industry Committee
Federation of American Hospitals
GlaxoSmithKline
Guidant Corporation
Healthcare Leadership Council
Hospira Worldwide, Inc.
Johnson & Johnson
Marshfield Clinic
McKesson Corporation
Medco Health Solutions, Inc.
Medical Group Management Association
Merck & Company, Inc.
National Association of Health Underwriters
National Association of Healthcare Access Management
National Association of Manufacturers
National Business Group on Health
Partners HealthCare System, Inc.
Pfizer, Inc.
Pharmaceutical Care Management Association
Premier, Inc.
Quest Diagnostics
Quintiles Transnational
Rx Benefits Coalition
Society for Human Resource Management
Tenet Healthcare Corporation
Texas Health Resources
Trinity Health
United States Chamber of Commerce
UnitedHealth Group
Vanderbilt University Medical Center
VHA Inc.
Wellpoint

cc: The Honorable Nancy Johnson

MR. DEAL. Thank you. Mr. Pyles.

MR. PYLES. Good afternoon, Mr. Chairman. I am pleased to be here. I am Jim Pyles, representing the American Psychoanalytic Association, and I would like to just associate my remarks a bit, I guess, with the remarks of Mr. Vaughan, who I think beautifully expressed the concerns of consumers, and those are largely the same concerns by our members because we found that psychotherapists are essentially the canaries in the coal mine when it comes to medical privacy. When there

is a threat to medical privacy you cannot provide effective psychotherapy. It just does not happen.

I have worked on this issue now for about 15 years, and I found that there is absolutely no end to the number of people who want to eliminate your medical privacy so they can help you. So I would urge you to think carefully about that. The fundamental question I think we have to ask ourselves as we look at a health IT system is are we going to compel Americans to disclose all of their most sensitive health information about themselves and their families into or from a national interoperable health information system without meaningful, informed patient consent, against their will, without adequate enforcement against unauthorized uses, disclosures, and just essentially disregarding their views.

One of the things I have not heard much of in the testimony today is what do the patients want, and I will be addressing that. I have learned in working on this issue that if you have no privacy, you have no liberty, and if you have no privacy, we do not have access to effective healthcare. It just does not happen. If Americans do not have a right to privacy to their innermost thoughts and their genetic makeup, what possible privacy could they have, what other things could be more private than that? What does meaningful consent and privacy mean? According to HHS it means the ability of individuals to determine for themselves when, how, and to what extent information about them is communicated. I think if you ask any person on the street they will have the same definition.

Courts have said it really is essentially the right to control the disclosure of your information, at least in some routine circumstances. Why is the right so important? Again, HHS concluded that in short the entire health delivery system is built upon the willingness of individuals to share the most intimate details of their lives with their healthcare providers. If that does not happen, an IT system is irrelevant, so that is the most significant concern when it comes to effective healthcare. HHS also concluded that unless public fears are allayed, it will be unable to obtain the full benefits of an electronic health information system. And yesterday former Speaker Newt Gingrich presented testimony before the Subcommittee on the Federal Work Gorce, and here is what he had to say about the patient's right to control their information: "Individuals have the right to control and must have the ability to control who can access their personal information." I could not agree with Mr. Gingrich more.

We know that we have sources already of national privacy standards. They appear in the Hippocratic Oath. It dates back to the 5th Century B.C., which is administered by 98 percent of the medical schools in this country to their graduates. We know that established standards for the

ethical practice of medicine adopted by every segment of the medical profession to essentially assure the patients that their information will not be disclosed without their consent. The AMA standard, for example, says, and I quote, "The physician should not reveal confidential communications or information without the express consent of the patient unless otherwise required to do so by law." We also know that this right to privacy for personal information is a fundamental concept of our system of government. It is embedded in the Fourteenth Amendment, the Fifth, the Fourth, and the First Amendments to the U.S. Constitution. This is the informational branch of the right to privacy, not the decisional branch where there is so much controversy. The Supreme Court is rock solid on protecting the right to informational privacy, and as I said, consent must be voluntary and it must be informed.

We also know that this right to privacy is grounded in the physician-patient privilege recognized in most States, including your own. The psychotherapist-patient privilege is recognized in all 50 States and the District of Columbia and in Federal common law. The right to privacy is also reflected in the tort laws and the statutory laws of all 50 States, and the States of Tennessee and California have the right to privacy in their State constitutions. We know also that the citizens of Georgia and the citizens of Ohio think pretty keenly about their right to privacy, and they have enacted a lot of laws to specifically protect it.

And if you look at tab two, which I will not go into, it lists the privacy laws in the State of Georgia that could be preempted by a bill such as H.R. 4157. Both of these States also recognize the private act of action which HIPAA does not. There are many other States that recognize similar privacy protections in areas of mental health information, genetic testing information, cancer diagnosis and treatment information, HIV/AIDS, drug and alcohol abuse diagnosis and treatment, birth defects, and many of these States give a private right of action. So I would urge you to be very careful about any bill that would preempt these laws the citizens of these States have said they need and want.

There are many other privacy protections under State law. Twenty-nine States now have breach protection or breach notification laws. I mentioned private rights of action are there. Let us look for a moment at the right of privacy under HIPAA. The HIPAA privacy rule really should be named a HIPAA disclosure rule because it provides regulatory permission for all covered entities and business associates to use and disclose identifiable health information for all routine purposes defined as treatment, payment, and healthcare operations, without notice to the patient, without the patient's consent over the individual's objection, even if the individual pays privately, and even retroactive to the

beginning of time, even information that was created prior to the compliance date.

Treatment, payment and healthcare operations, the reason for which this information can be disclosed without permission is a lengthy list. If you look at tab four you will see that list of purposes. HHS responded to many of the concerns that consumers had in adopting that regulation by saying it was only a floor, that still practitioners could still obtain consent, that more stringent laws remain in effect, and that ethical standards retain their vitality. I would urge you that with any law that you are thinking of today you preserve those protections. What does the public want and expect? If you look at HHS' findings they have found that the public has a common belief and strong expectation that their identifiable information will not be disclosed without their consent. Sixty-five percent of Americans would not disclose sensitive information and necessary information to their physicians and providers if they thought it would go into the electronic record.

Seventy-five percent are concerned about the loss of medical privacy due to the use of electronic information, and we know that this concern translates into adverse effects on healthcare. Six hundred thousand people a year according to HHS, 600,000 people a year, do not seek early diagnosis and treatment for cancer, 2 million more annually do not seek needed treatment for mental illness. Thousands do not seek treatment for sexually transmitted diseases. One in six Americans takes evasive actions to avoid privacy violations, including providing inaccurate information, changing physicians or avoiding healthcare altogether, and 87 percent of physicians report withholding information from a patient's medical record due to privacy concerns.

So we would urge you to start this process with strong privacy protections. Also, we know that an IT system poses a greater threat to health information privacy. The President's Information Technology Advisory Committee concluded that the Nation's electronic information systems are highly vulnerable to corruption by hackers and others, that the threat is growing by over 20 percent annually, and the increasing vulnerabilities cannot be addressed by current technology.

MR. DEAL. May I ask you to summarize rather quickly, please?

MR. PYLES. I will. In conclusion, I would just like to say that the the right course of action for Congress to take, I believe, is ground any health IT system in strong privacy protections reflected in the history of the Nation in its medical and professional standards, the law of psychotherapy patient privilege, and the constitutional common law provide for meaningful, informed patient consent, provide a private right of action, and prompt notification for any breaches. Lastly, I would just mention the concern for the loss of medical privacy should be a

particular concern for Members of this body because under the Supreme Court's decision in 2001, Bartnicki v. Vopper, the court held that information about a public official or a public event which is obtained, even if it is obtained unlawfully, can be published by the press and the press has a First Amendment right to do it, and Congress cannot prevent that publication.

So we know these electronic information systems cannot be rendered secure. It is very likely that elections in the future are going to turn on what is in a politician's medical record as well as his talents he brings to the table. Thanks very much.

[The prepared statement of James C. Pyles follows:]

PREPARED STATEMENT OF JAMES C. PYLES, ATTORNEY MEMBER, POWES, PYLES, SUTTER AND VERVILLE, P.C.

SUMMARY OF TESTIMONY BEFORE THE HOUSE COMMITTEE ON ENERGY AND COMMERCE SUBCOMMITTEE ON HEALTH

"Legislative Proposals to Promote Electronic Health Records And a Smarter Health Information System"

Testimony of James C. Pyles, Counsel
American Psychoanalytic Association
March 16, 2006

The entire health delivery system is dependent upon the willingness of individuals to share the most intimate details of their lives with their health care practitioners. A national "interoperable" electronic health information system is unlikely to be accepted by the public and be successful unless it is built upon traditional standards of medical privacy that the public expects and that are part of the standards for the ethical practice of medicine and psychiatry.

The right to medical privacy is widely accepted as the right of the individual to have some control over the disclosure of his or her identifiable health information in most routine situations. This right has been identified throughout the history of medicine and the history of the our nation as essential for quality health care. The right finds its source in the Hippocratic Oath, established standards of medical ethics, the amendments of the Bill of Rights and the 14th Amendment to the U.S. Constitution, the physician-patient and psychotherapist-patient privilege, and the statutory and common law of every state.

The right to privacy and consent was not recognized and protected in the HIPAA Amended Privacy Rule implemented on April 14, 2003. However, the Department of Health and Human Services explained in issuing the rule that it was only intended as a "floor" of privacy protections and that it was not intended to preempt more protective state privacy laws nor override established standards of medical ethics.

The public wants strong health information privacy protections preserved and fears that a national electronic health information system will eliminate the right to privacy and consent. Any electronic health information legislation should be built on the privacy principles reflected in standards of medical ethics, the law of medical privilege, constitutional common law, and state laws. There should be no preemption of state laws unless and until Congress enacts strong national health information privacy standards and principles.

James C. Pyles
Powers, Pyles, Sutter, & Verville, P.C.
1875 Eye Street, NW
Washington, D.C. 20006
(202) 466-6550
jim.pyles@ppsv.com

WILL A NATIONAL "INTEROPERABLE" HEALTH INFORMATION SYSTEM PRESERVE OR ELIMINATE THE PATIENT'S RIGHT TO HEALTH INFORMATION PRIVACY?

Health Subcommittee of House Committee on
Energy and Commerce
March 16, 2006

James C. Pyles
Counsel
American Psychoanalytic Association

I. **Fundamental question presented by health IT bills**—Will Congress **compel Americans** to disclose all of their most sensitive health information about themselves and their families to and from a national "interoperable" health information system **without meaningful, informed patient consent, against their will and without adequate enforcement against unauthorized uses and disclosures?**

A. Without a right to **privacy**, there can be no **liberty**, and Americans will not have access to **quality health care**.

B. If Americans' privacy for their **inner-most thoughts** and their **genetic make-up** is not protected, they will not seek treatment or support the use of electronic health records.

II. **What does meaningful consent and privacy mean?**

A. HHS--The ability of individuals "to **determine for themselves** when, how, and to what extent information about them is communicated." [1]

B. Courts—**"control over knowledge about one's self**...one of the most **fundamental and cherished** rights of American citizenship, falling within the right

[1] 65 Fed. Reg. at 82,465.

characterized by Justice Brandeis as 'the right to be let alone'." [2]

III. Why is the right to health information privacy important?

A. HHS Findings--

i. "In short, the **entire health care system** is built upon the willingness of individuals to share the most intimate details of their lives with their health care providers." [3]

ii. "While privacy is one of the key values on which our society is built, it is more than an end in itself. It is also necessary for the **effective delivery of health care**, both to individuals and to populations." [4]

iii. "Unless public fears are allayed, we will be **unable to obtain the full benefits of electronic technologies.** The absence of national standards for the confidentiality of health information has made the health care industry and the population in general uncomfortable about this **primarily financially-driven expansion** in the use of electronic data." [5]

IV. Sources of the nationally and locally recognized right to meaningful consent and health information privacy.

A. The **Hippocratic Oath** dating from the 5th Century B.C. which is administered to graduates by 98% of the medical schools in the U.S. and Canada. [6]

---

[2] U.S. v. Westinghouse, 638 F.2d 570, 576, 577, n. 5 (3rd Cir. 1980).
[3] 65 Fed. Reg. at 82,467.
[4] 65 Fed. Reg. at 82,467.
[5] 65 Fed. Reg. at 82,466..
[6] "The Use of the Hippocratic Oath", R. Orr, M.D. and N. Pang, M.D.

B. **Established standards for the ethical practice of medicine** adopted by every segment of the medical profession which state that

1. "The physician **should not reveal confidential communications or information** without the express consent of the patient, unless otherwise required to do so by law." [7]

C. The **Fourteenth, Fifth, Fourth, and First Amendments to the U.S. Constitution**—this is the **"informational"**, rather than the "decisional" branch, of the right to privacy which the Supreme Court has consistently found provides that an individual's personal health information may not be disclosed without his or her consent unless there is a **"compelling" governmental interest,** and even then the government must use the **"least intrusive alternative".** [8]

1. Consent must also be **voluntary and informed.** [9]

D. **The physician-patient privilege** recognized in most states. [10]

E. **The psychotherapist-patient privilege**—recognized in all 50 states and the District of Columbia and in Federal common law. [11]

F. **Tort laws or statutory laws** in all 50 states recognize a right to privacy. Some states, like **Tennessee and California** have an explicit right to privacy in their State Constitutions. [12]

---

[7] See Principles of Medical Ethics of the American Medical Association and many other medical associations and societies in Tab 1.

[8] Ferguson v. City of Charleston, 532 U.S. 67; Whalen v. Roe, 429 U.S. 589 (1977); Sell v. United States, 539 U.S. 166, 181 (2003); Tucson Woman's Clinic v. Eden, 371 F. 3d 1173 (9th Cir. 2004).

[9] Ferguson v. City of Charleston, 308 F.3d 380, 399 (4th Cir. 2002).

[10] Northwestern Mem. Hosp. v. Ashcroft, 362 F.3d 923 (7th Cir. 2004).

[11] See Jaffee v. Redmond, 518 U.S. 1 (1996).

[12] 65 Fed. Reg. at 82,464.

G. **State laws, in Georgia and Ohio**, for example, provide privacy protections for health information held by health care facilities, physicians, pharmacists, and long term care facilities, as well as special protections for **alcohol and drug abuse, genetic testing, HIV/AIDS, mental health, sexually transmitted disease, cancer and birth defect information** as well as provide a **private right of action** for violations. [13]

H. Health information **currently has privacy protection** under **most state laws** that is not provided by the HIPAA Privacy Rule

   i. Mental health information

   ii. Genetic testing information

   iii. Cancer diagnosis and treatment information

   iv. HIV/AIDS testing and treatment information

   v. Drug and alcohol abuse diagnosis and treatment information

   vi. Birth defect information [14]

   vii. At the state level, specific patient authorization is often required before this type of sensitive health information can be disclosed.

I. **Other privacy protections** recognized under state law.

   i. Privacy breach **notification** —29 states now have these laws

   ii. **Private right of action** [15]

---

[13] See list of Georgia and Ohio health information privacy laws summarized in Tab 2.
[14] See summaries of these laws for the states of Georgia and Ohio.

iii. **Physician-patient privilege** statutes and common law—recognized in most states [16]

iv. **Psychotherapist-patient privilege** laws—recognized in all 50 states and the District of Columbia [17]

v. The right to privacy and consent under an **implied contract** between physicians and patients [18]

V. The right to privacy under HIPAA

A. HIPAA Privacy **Rule**— provides **"regulatory permission" for all covered entities** and business associates to use and disclose identifiable health information for all routine purposes (**treatment, payment and health care operations**): [19]

i. without **notice**

ii. without **consent**

iii. over the individual's **objection**

iv. even if the individual **pays privately**

v. even information **prior to the compliance date** [20]

B. **Treatment, payment, and health care operations** include nearly 100 uses that **broadly eliminate** the individual's right to health information privacy. [21] In short,

---

[15] Both Georgia and Ohio permit a private right of action for breaches of health information privacy under state law. Tab 2.
[16] Northwestern Mem. Hosp. v. Ashcroft, 362 F.3d 923 (7th Cir. 2004).
[17] Jaffee v. Redmond, 518 U.S. 1 (1996).
[18] Givens v. Millikin, 75 S.W. 3d 383 (Tenn. 2002).
[19] 67 Fed. Reg. at 53,211 Tab 3.
[20] 45 C.F.R. 164.506(a) (amended) Tab 3.
[21] See list of uses included in treatment, payment and health care operations at Tab 4.

patients have no meaningful right to control their own health information.

C. **HHS response to comments** that the privacy rule **violates state law and medical ethics**

1. The HIPAA Privacy Rule is **only a "floor"** of protections, they are **not even** to serve as a **"best practices"** standard;

2. The HIPAA Privacy Rule still **"permits"** covered entities – providers and health plans to obtain consent; (need to give examples of who's left out)

3. **More stringent (protective) state laws** (such as those mentioned above) are not weakened or preempted; and

4. **Ethical standards** retain "their vitality". [22]

D. **Other problems magnified** by the Rule

i. Privacy protections apply **only to** covered entities which include **only** providers, health plans and healthcare clearinghouses and not others who handle health information;

ii. **No notice** requirement for privacy breaches;

iii. **No accounting** for routine disclosures;

iv. **Weak enforcement** provisions—over 17,000 complaints of privacy violations but only one enforcement action since April 14, 2003. [23]

v. No **private right of action.**

---

[22] 67 Fed. Reg. at 53,212 Tab 3.
[23] Office of Civil Rights quoted in Reading Eagle (Feb. 24, 2006)

VI. What does the public expect and want?

A. HHS—Public has a **"common belief"** and **"strong expectation"** that their identifiable health information will not be disclosed without their consent. [24]

B. Supreme Court—Patients have a **"reasonable expectation"** that diagnostic tests will not be shared with non-medical personnel without their consent. [25]

C. **65% of Americans** would not disclose sensitive but necessary information to their physicians and providers if they thought it would go into an electronic health information system. [26]

D. **75% of Americans** are concerned about the loss of medical privacy due to the use of an electronic health information system. [27]

E. **63% of Americans** would not take a genetic test if the results were communicated to their insurers or employers, [28]

F. **35% of people** offered a free genetic test to access the risk of breast cancer declined citing loss of privacy concerns. [29]

G. **Adverse effects** of privacy concerns on patients:
   i. approximately **600,000 people** annually do not seek early diagnosis and treatment for cancer,

---

[24] 65 Fed. Reg. at 82,472.
[25] Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001).
[26] Report of study by Center for Social and Legal Research presented to the National Committee on Vital and Health Statistics, by Dr. Alan Westin, Professor of Public Law & Government, Columbia University (February 23, 2005).
[27] Ethics Survey of Consumer Attitudes about Health Web Sites, California Health Care Foundation , at 3 (January 2000).
[28] 65 Fed. Reg. at 82,466.
[29] Id.

ii. more than **2 million people** annually do not seek needed treatment for mental illness,

iii. **many people** do not seek treatment for sexually transmitted diseases, [30]

iv. "**one in six Americans** take evasive action to avoid privacy violations including providing inaccurate information, changing physicians, or avoiding health care altogether." [31]

v. **87% of physicians** report withholding information from a patient's medical record due to privacy concerns. [32]

VII. A health IT system poses a greater threat to health privacy.

A. HHS—"In a matter of seconds, a person's most profoundly private information can be shared with **hundreds, thousands, even millions of individuals and organizations at a time....**[eliminating] many of the financial and logistical obstacles that previously served to protect the confidentiality of health information and the privacy interests of individuals." [33]

B. Health IT creates the potential for breaches of health information privacy on **a scale previously unimaginable.**[34]

C. Once health information is disclosed electronically, it **cannot be recovered.**

---

[30] 65 Fed. Reg. at 82,778.
[31] 65 Fed. Reg. at 82,468.
[32] Id.
[33] 65 Fed. Reg. at 82,465.
[34] "Theft Nabs Backup Data on 365,000 Patients", Computerworld (January 26, 2006)

D. HHS—"there is **no such thing** as a totally secure [electronic information] system that carries no risk". [35]

E. Findings of the **President's Information Technology Advisory Committee:**

i. the nation's electronic information systems are **"highly vulnerable"** to corruption by hackers and others;

ii. "the threat is clearly growing" with attacks rising by **"over 20 percent annually"**;

iii. the increasing **vulnerabilities cannot be addressed** by the current "patching" approach, and new research is needed "to design security into computing and networking systems and software from the ground up." [36]

VIII. Concerns with H.R. 4157 – Overall – patients want meaningful control and adequate enforcement. This bill does not accomplish either.

A. It authorizes the Secretary to issue a **"single set of national standards"** for the privacy of health information.

B. And it allows the Secretary to **preempt privacy protections in State laws** "to the extent **the Secretary determines**" such standards are "necessary to promote uniformity and efficiency". Section 4(b)(1). The study fails to assess existing national privacy standards and why certain state laws are in place and what value they have for patients.

C. **Given Congress' past inability** to reach agreement on key issues, the process is virtually guaranteed to result in

[35] 68 Fed. Reg.at 8,346.
[36] "Cyber Security: A Crisis in Prioritization", President's Information Technology Advisory Committee, at 7-12 (February 23, 2005).

the Secretary of HHS setting the national privacy standard.

D. **Unelected government officials**, such as the Secretary of HHS, should not be given **the power to eliminate "fundamental and cherished" rights** of citizens.

IX. The right course of action for Congress

A. Ground any health IT system in the **strong privacy standards reflected in the history of the nation** in professional and medical ethics, the law of medical and psychotherapy privilege, federal and state law, and constitutional common law.

B. Provide for **meaningful, informed patient consent** which allows patients some control over whether their health information is shared over a national health network and what information may be shared.

C. **Bring the "floor" of privacy protections in the HIPAA Privacy Rule** into conformity with existing national privacy standards and citizens' expectations.

D. Provide health information privacy protections that apply **to anyone** who handles the information.

E. Provide for **prompt notification** of the individual and the Secretary of any actual or suspected privacy breach and require the Secretary to maintain a **publicly accessible list** of organizations that have had privacy breaches and the remedial action taken.

F. Require an **electronic audit trail** for the disclosure of all health information.

G. Provide for **electronic segregation** of highly sensitive health information into more secure electronic sites.

H. Provide for individuals to be able **to opt in or opt out** of such systems fully or with respect to certain information.

I. Provide strong protections to prevent **employers** from gaining access to their employees' health information.

J. Provide for a **private right of action** to obtain injunctive relief and damages for privacy breaches.

X. Finally, there is the **Bartnicki** problem.

A. According to the Supreme Court, the media has a First Amendment **right to publish** information about any matter of "public or general interest" **even if that information is obtained unlawfully.** Bartnicki v. Vopper, 532 U.S. 514, 534 (2001).

B. Thus, any health information obtained by someone hacking into an electronic health information system could be **published on the front page of the Washington Post** if it concerned a public official.

C. This could include **any member of the Administration or Congress,** members of state administrations and legislatures, state and local boards, officials of political parties.

D. Congress **could not pass a law** to prevent that publication.

E. Under an electronic health information system with the HIPAA privacy protections, it is **unlikely that Presidents Kennedy or Reagan would have ever reached the White House.**

F. Unless the strongest possible privacy protections are included in any health IT bill, **federal and state elections** in the future will be determined by the content of the candidates' medical records.

James C. Pyles
Powers, Pyles, Sutter and Verville, P.C.
1875 Eye Street, 12th Floor
Washington, D.C. 20006
(202) 466-6550
jim.pyles@ppsv.com

On behalf of the American Psychoanalytic Association

FINDINGS AND FACTS IN SUPPORT OF ETHICS BASED MEDICAL PRIVACY

(1) **The entire health delivery system** is based upon the willingness of the individual to trust a health care practitioner sufficiently to disclose to the practitioner the most intimate details of his or her life.[1]

(2) An assurance of **privacy** of health information is **necessary to secure effective, high quality health care.**[2]

(3) The "**reason and experience**" of the country shows that effective psychotherapy is dependent an atmosphere of trust confidence and trust in which the patient is willing to make a frank and complete disclosure of facts, emotions, memories and fears without fear of nonconsensual uses and disclosures.[3]

(4) Adequate protection of the **security and privacy** of health information is a ***sine qua non* of the increased efficiency of information exchange brought about by the electronic revolution.**[4]

(5) Citizens have a **reasonable expectation** that their most intimate identifiable health information will not be used and disclosed in routine situations without their consent or over their objections.[5]

(6) The public is **increasingly concerned** about the loss of personal privacy due to the increasing use of **interconnected electronic information systems** which make it possible in a matter of seconds to share a person's most profoundly private information with hundreds, thousands, and even millions of individuals and organizations.[6]

(7) A recent study found that **70% of the public is concerned that their health information will be leaked or shared without their**

---

[1] See 65 Fed. Reg. at 82,467, finding of the U.S. Department of Health and Human Services in issuing the Original Standards for Privacy of Individually Identifiable Health Information after one of the most extensive rulemaking proceedings in the history of the department. This HHS finding, as well as those listed below, were confirmed by HHS when the Original Privacy Rule was put into effect without change by the current Administration (66 Fed. Reg. at 12,434). None of these findings was retracted when the Original Rule was amended on August 14, 2002 (67 Fed. Reg. 53,182).
[2] 65 Fed. Reg. at 82,467.
[3] Jaffee v. Redmond, 116 S. Ct. 1923, 1928 (1996).
[4] 65 Fed. Reg. at 82,474.
[5] Ferguson v. City of Charleston, 121 S. Ct. 1281, 1288 (2001); Statement of Massachusetts Medical Society, "Patient Privacy and Confidentiality" (1996); finding by HHS (65 Fed. Reg. at 82,472).
[6] 65 Fed. Reg. at 82,465.

permission by an electronic health information system.[7] It also found that **65% of Americans would not disclose sensitive but necessary health information to doctors and health care providers** because of worries that the information will go into an electronic health information system.[8] This is consistent with HHS' earlier findings that annually **600,000 citizens** do not seek early diagnosis and treatment for cancer, **2 million citizens** do not seek treatment for mental illness and **thousands of citizens** do not seek treatment for sexually transmitted diseases due to privacy concerns. [9]

(8) The privacy of identifiable health information depends in large part on the existence of security measures to prevent unwanted disclosures. However, **there is no such thing as a totally secure electronic information system.**[10]

(9) The nation's electronic information systems are **highly vulnerable** to unauthorized intrusion, the attacks and **vulnerabilities are growing** rapidly, and they cannot be addressed adequately with current technology.[11]

10) Federal agencies have taken **even fewer measures** than the private sector to identify and address the growing threats to cyber security.[12]

11) Privacy is a **fundamental right.**[13]

12) **All fifty states** today recognize in tort law a common law or statutory right to privacy. Some states, such as Tennessee and California, have a right to privacy as a matter of **state constitutional law.**[14]

13) Many of the most basic protections in the Constitution of the United States are imbued with an attempt to protect individual privacy while balancing it against larger societal purposes of the nation. The right to privacy is reflected in the **First Amendment's** protection of freedom of religion, the **Second Amendment's** protection of the right to keep and bear arms, the **Third Amendment's** protection of the right to not have

---

[7] Testimony of Dr. Alan F. Westin, Professor of Public Law & Government Emeritus, Columbia University at Hearing on Privacy and Health Information Technology before the NCVHS Subcommittee on Privacy, at 5, (February 23, 2005).
[8] Id.
[9] 65 Fed. Reg. at 82,778.
[10] 68 Fed. Reg. at 8,335, 8,346.
[11] "Cyber Security: A Crisis of Prioritization: Report to the President", President's Information Technology Advisory Committee, 5-12 (February 28, 2005).
[12] "Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems", General Accountability Office, GAO-05-231, at 6 (May 13, 2005).
[13] 65 Fed. Reg. at 82,464 (December 28, 2000).
[14] Id.

soldiers quartered in one's house without consent, the **Fourth Amendment's** protection against unreasonable searches and seizures, the **Fifth and Fourteenth Amendments'** protection of the right to Liberty, and the **Ninth Amendment's** protection of rights retained by the people.[15]

14) The **right to privacy** is "the claim of individuals, groups, or institutions to determine for themselves, **when, how, and to what extent** information about them is communicated."[16]

15) **The Hippocratic Oath**, since the 5th century B.C., has recognized that physicians have a duty to keep patient information confidential. The Oath has remained in Western Civilization as an expression of ideal conduct for the physician.[17] The Oath is administered to the graduates of 98% of the medical schools in the United States and Canada.[18]

16) **Current standards of medical ethics** of virtually every segment of the medical profession provide that identifiable health information should not be disclosed without the patient's informed consent:

a. **The American Medical Association**: "A physician shall...safeguard patient confidences within the constraints of the law."

   "The physician should not reveal confidential communications or information without the express consent of the patient, unless required to do so by law."[19]

b. **The American College of Physicians—American Society of Internal Medicine**: "Confidentiality is a fundamental tenet of medical care...The physician must not release information without the patient's consent (often termed a 'privileged communication')."[20]

c. **The Association of American Physicians and Surgeons**: "The special importance of the patient's privacy in medical matters requires that the physician never reveal either the confidence entrusted to him in the course of medical

---

[15] Id.
[16] A. Cavoukian, D. Tapscott, "Who Knows: Safeguarding Your Privacy in a Networked World," Random House (1995).
[17] American Medical Association, Code of Medical Ethics, History (2001).
[18] R. Orr, M.D., and N. Pang, M.D., The Use of the Hippocratic Oath: A Review of 20th Century Practice and a Content Analysis of Oaths Administered in Medical Schools in the U.S. and Canada in 1993.
[19] American Medical Association, Principles of Medical Ethics, IV; Current Opinions of the Council on Ethical and Judicial Affairs, E-5.05 (1998).
[20] American College of Physicians—American Society of Internal Medicine, Ethics Manual (1998).

attendance, or deficiencies he may observe in the character of the patient, releasing information only with the consent of the patient and with due consideration of the mandates of law.[21]

d. **The American Dental Association:** "The dentist has a duty to respect the patient's rights to self-determination and confidentiality."

   "Dentists are obligated to safeguard the confidentiality of patient records."[22]

e. **The American Academy of Physical Medicine and Rehabilitation:** "Patient confidentiality must be respected at all times. This includes confidentiality of the medical records. Patient's privacy should be honored unless mandated by law. Consent of the patient or other responsible party should be obtained for release of information."[23]

f. **The American Nursing Association:** "The nurse safeguards the patient's right to privacy. The need for health care does not justify unwanted intrusion into a patient's life. The nurse advocates for an environment that provides for sufficient physical privacy, including auditory privacy for discussions of a personal nature and policies and practices that protect the confidentiality of information.

   Associated with the right to privacy, the nurse has a duty to maintain confidentiality of all patient information. The patient's well-being could be jeopardized and the fundamental trust between the patient and the nurse destroyed by unnecessary access to data or by the inappropriate disclosure of identifiable patient information."[24]

g. **The American Psychiatric Association:** "A physician shall respect the rights of patients, colleagues, and other health professionals, and shall safeguard patient confidences and privacy within the constraints of the law. Psychiatric records, including even the identification of a person as a patient, must be protected with extreme care.

---

[21] Association of American Physicians and Surgeons, Principles of Medical Ethics, (9) (January 1991).
[22] American Dental Association, Principles, Code of Professional Conduct and Advisory Opinions, Section 1.
[23] American Academy of Physical Medicine and Rehabilitation, Code of Conduct, II. Ethics Relating to the Patient and the Patient's Family.
[24] American Nursing Association, Code of Ethics, 3.1, 3.2.

Confidentiality is essential to psychiatric treatment. This is based in part on the special nature of psychiatric therapy as well as on the traditional ethical relationship between physician and patient. Growing concern regarding the civil rights of patients and the possible adverse effects of computerization, duplication equipment, and data banks makes the dissemination of confidential information an increasing hazard....

A psychiatrist may release confidential information only with the authorization of the patient or under proper legal compulsion."[25]

h. **The American Psychoanalytic Association**: "Confidentiality of the patient's communications is a basic patient's right and an essential condition for effective psychoanalytic treatment and research...

All information about the specifics of a patient's life is confidential, including the name of the patient and the fact of treatment. The psychoanalyst should resist disclosing confidential information to the full extent permitted by law....

The psychoanalyst should never share confidential information about a patient with nonclinical third-parties (e.g. insurance companies) without the patient's or, in the case of a minor patient, the patient's or guardian's informed consent."[26]

i. **The American Psychological Association**: "Psychologists have a primary obligation and take reasonable precautions to protect confidential information obtained through or stored in any medium, recognizing that the extent and limits of confidentiality may be regulated by law or established by institutional rules or professional or scientific relationship....

Psychologists may disclose confidential information with the appropriate consent of the organizational client, the individual client/patient, or another legally authorized person on behalf of the client/patient unless prohibited by law.

Psychologists disclose confidential information without the consent of the individual only as mandated by law, or where permitted by law for a valid purpose such as to (1) provide needed professional services; (2) obtain appropriate

[25] American Psychiatric Association, Principles of Medical Ethics with Annotations Especially Applicable to Psychiatry, Section 4 (2001).
[26] American Psychoanalytic Association, Principles and Standards of Ethics for Psychoanalysts, General Guiding Principles, IV., Standards Applicable to the Principles of Ethics for Psychoanalysts, IV.2.

professional consultations; (3) protect the client/patient, psychologist, or others from harm; or (4) obtain payment for services from a client/patient, in which instance disclosure is limited to the minimum that is necessary to achieve the purpose."[27]

j. **The National Association of Social Workers**: "Social workers should respect clients' right to privacy. Social workers should not solicit private information from clients unless it is essential to providing services or conducting social work evaluation or research. Once private information is shared, standards of confidentiality apply....

   Social workers may disclose confidential information when appropriate with valid consent from a client or a person legally authorized to consent on behalf of a client.[28]

k. **Clinical Social Work Federation**: "Clinical social workers have a primary obligation to maintain the privacy of both current and former clients, whether living or deceased, and to maintain the confidentiality of material that has been transmitted to them in any of their professional roles. Exceptions to this responsibility will occur only where there are overriding legal or professional reasons and, whenever possible, with the written and informed consent of the client(s)."[29]

l. **American College of Emergency Room Physicians**: "The principles listed below express fundamental moral responsibilities of emergency physicians....

   Emergency physicians shall...Respect patient privacy and disclose confidential information only with consent of the patient or when required by an overriding duty such as the duty to protect others or to obey the law."[30]

m. **American Physical Therapy Association**: "Information relating to the physical therapist/patient relationship is confidential and may not be communicated to a third party not involved in that

[27] American Psychological Association, Ethical Principles of Psychologists and Code of Conduct, Ethical Standards, Maintaining Confidentiality, 4.01, Disclosures, 4.05 (June 1, 2003).
[28] National Association of Social Workers, Ethical Standards, 1.07 Privacy and Confidentiality (1999).
[29] Clinical Social Work Federation, Code of Ethics, III. Confidentiality (2003).
[30] American College of Emergency Room Physicians, Code of Ethics, Principles of Ethics for Emergency Physicians, 5 (October 2001).

patient's care without the prior consent of the patient, subject to applicable law."[31]

n. **American Society of Radiologic Technologists**: "The radiologic technologist respects confidences entrusted in the course of professional practice, respects the patient's right to privacy and reveals confidential information only as required by law or to protect the welfare of the individual or the community.[32]

o. **American Pharmacy Association**: "This Code, prepared and supported by pharmacists, is intended to state publicly the principles that form the fundamental basis of the roles and responsibilities of pharmacists. These principles, based on moral obligations and virtues, are established to guide pharmacists in relationships with patients, health professionals, and society.[33]

   A pharmacist is dedicated to protecting the dignity of the patient. With a caring attitude and a compassionate spirit, a pharmacist focuses on serving the patient in a private and confidential manner.

p. **National Community Pharmacists Association**: "NCPA strenuously opposes electronic prescription transmission programs or manufacturers' marketing program, such as patient information or poverty relief, that violate the integrity and confidentiality of the face-to-face relationship between the patient and the community pharmacist. NCPA supports explicit patient medical releases that prevent patient-specific data from being extracted, provided, or sold to extraneous parties without the informed and express written consent of the patient.[34]

17) Standards of medical ethics define **moral principles** for the practice of medicine. **Unethical conduct** in the practice of medicine is professional conduct that fails to conform to these moral standards or policies.[35]

18) As a matter of medical ethics and constitutional principles deeply rooted in the nation's history and tradition, law abiding citizens who

---

[31] American Physical Therapy Association, APTA Guide for Professional Conduct, Ethical Principle, 2.3 Confidential Information (January 2004).
[32] American Society of Radiologic Technologists and the American Registry of Radiologic Technologists, Code of Ethics, (9) (February 2003).
[33] American Pharmacy Association, Code of Ethics for Pharmacists, Preamble and Section II.
[34] National Community Pharmacists Association, Patient Confidentiality/Privacy, Position Statement.
[35] American Medical Association, Current Opinions of the Council on Ethics and Judicial Affairs, E-1.01 Terminology (June 1996).

pose no health threat to society should not have their intimate health information used or disclosed without notice, without their consent or over their objection and should not be compelled or coerced to disclose their identifiable health information to an electronic health information system that cannot guarantee the privacy of that information.

Georgia Health Information Privacy Laws

1. **HMOs**

   HMOs may not disclose any information pertaining to diagnosis, treatment or health of any enrollee or applicant or information from any provider without the patient's or applicant's express consent. Ga. Code Ann. 33-21-23.

2. **Physicians, hospitals, health care facilities and pharmacies**

   Physicians, hospitals, health care facilities and pharmacists generally may not be required to release any medical information concerning a patient accept upon written authorization. Ga. Code Ann. 24-9-40.

3. **Insurance entities**

   Generally, an insurance entity may not disclose medical information about a person it collected or received in connection with an insurance transaction without that person's written authorization. Ga. Code Ann. 33-39-14.

4. **Residents of long term care facilities**

   Residents of long term care facilities have a right to privacy in their medical, personal and bodily care programs. Case discussions, consultations, examinations, treatments, and care are confidential and are to be conducted in privacy. Ga. Code Ann. 31-8-114(6).

5. **Genetic testing**

   Information derived from genetic testing is confidential and may be released only to the individual tested and to persons specifically authorized by such individual in writing. Ga. Code Ann. 33-54-3.

6. **HIV/AIDS**

A person or entity that is responsible for recording, reporting, or maintaining AIDS confidential information or that receives that information as permitted by law may not intentionally or knowingly disclose that information to another. Ga. Code Ann. 24-9-47(b).

7. Mental health records

Mental health records may not be released except with patient authorization and in several other limited circumstances. Ga. Code Ann. 37-3-166.

8. Privileges

Psychotherapy communications and information are subject to a psychotherapist-patient privilege which applies to patients of psychiatrists, licensed psychologists, licensed clinical social workers, licensed marriage counselors and others who render psychotherapy. Ga. Code Ann. 24-9-21.

9. Private right of action

A private right of action is available for privacy violations by insurance companies and HMOs [Ga. Code Ann. 33-39-22] and for the improper disclosure of genetic testing information [Ga. Code Ann. 33-54-8].

Ohio Health Information Privacy Laws

1. **Health Insuring Corporation**

   Health information pertaining to an individual's treatment or health obtained by a health insuring corporation from the individual or any health care facility must be held in confidence and may not be disclosed without the express consent of the individual, with several limited exceptions. Oh. Rev. Code 1751.52.

2. **Insurance entities including health insuring corporations**

   Generally, an insurance entity may not disclose medical information about a person that it collected or received in connection with an insurance transaction without that person's written authorization. Oh. Rev. Code 3904.13.

3. **Nursing home residents**

   Nursing home residents have a right to confidential treatment of personal and medical records, and the right to approve or refuse the release of their records to any individual outside the home, with limited exceptions. Oh. Rev. Code 3721.13.

4. **Physicians, physicians assistants and psychologists**

   Physicians and physicians' assistants who betray a professional confidence can be brought before the State Medical Board for disciplinary action. Oh. Rev. Code 4730.25(B)(7); 4731.22(B)(4). The same is true for psychologists who make unauthorized disclosures of information received in confidence. Oh. Rev. Code 4732.17.

5. **Birth defects**

   Records and information concerning birth defects are confidential and may not be disclosed without the written

consent of the child's parent or legal guardian, with limited exceptions. Oh. Rev. Code 3705.32.

6. Genetic test results

Insurers and health insuring corporations may not require, consider, or inquire into the results of genetic screening or testing in processing an application for insurance coverage. Oh. Rev. Code 1751.64; 3901.49; 3901.50.

7. HIV/AIDS

No person who acquires HIV-related information while providing any health care service or while employed by a health care provider or facility may disclose the identity of any individual on whom an HIV test is performed, the results of the test, or the identity of any person diagnosed as having AIDS or an AIDS related condition without the written authorization of the individual. Oh. Rev. Code 3701.243(A).

8. Privileges

Ohio recognizes a privilege protecting communications between patients and physicians, dentists, chiropractors, school guidance counselors, professional counselors and social workers and psychologists. Oh. Rev. Code 2317.02(B)(1), 2317.02(J)(1), 2317.02(G)(1), and 4732.19.

9. Private right of action

A private right of action exists for unauthorized disclosures of health information by insurers and health insuring corporations [Oh. Rev. Code 3904.2] and for the unauthorized disclosure of HIV/AIDS information [Oh. Rev. Code 3701.244].

The Department adopts the approach that was proposed in the NPRM, because it is the only one that resolves the operational problems that have been identified in a simple and uniform manner. First, this Rule strengthens the notice requirements to preserve the opportunity for individuals to discuss privacy practices and concerns with providers. (See section III.H. of the preamble for the related discussion of modifications to strengthen the notice requirements.) Second, the final Rule makes the obtaining of consent to use and disclose protected health information for treatment, payment, or health care operations optional on the part of all covered entities, including providers with direct treatment relationships. A health care provider that has a direct treatment relationship with an individual is not required by the Privacy Rule to obtain an individual's consent prior to using and disclosing information about him or her for treatment, payment, and health care operations. They, like other covered entities, have regulatory permission for such uses and disclosures. The fact that there is a State law that has been using a similar model for years provides us confidence that this is a workable approach.

Other rights provided by the Rule are not affected by this modification. Although covered entities will not be required to obtain an individual's consent, any uses or disclosures of protected health information for treatment, payment, or health care operations must still be consistent with the covered entity's notice of privacy practices. Also, the removal of the consent requirement applies only to consent for treatment, payment, and health care operations; it does not alter the requirement to obtain an authorization under § 164.508 for uses and disclosures of protected health information not otherwise permitted by the Privacy Rule or any other requirements for the use or disclosure of protected health information. The Department intends to enforce strictly the requirement for obtaining an individual's authorization, in accordance with § 164.508, for uses and disclosure of protected health information for purposes not otherwise permitted or required by the Privacy Rule. Furthermore, individuals retain the right to request restrictions, in accordance with § 164.522(a). This allows individuals and covered entities to enter into agreements to restrict uses and disclosures of protected health information for treatment, payment, and health care operations that are enforceable under the Privacy Rule.

Although consent for use and disclosure of protected health information for treatment, payment, and health care operations is no longer mandated, this Final Rule allows covered entities to have a consent process if they wish to do so. The Department heard from many commenters that obtaining consent was an integral part of the ethical and other practice standards for many health care professionals. It, therefore, does not prohibit covered entities from obtaining consent.

This final Rule allows covered entities that choose to have a consent process complete discretion in designing that process. Prior comments have informed the Department that one consent process and one set of principles will likely be unworkable. Covered entities that choose to obtain consent may rely on industry practices to design a voluntary consent process that works best for their practice area and consumers, but they are not required to do so.

This final Rule effectuates these changes in the same manner as proposed by the NPRM. The consent provisions in § 164.506 are replaced with a new provision at § 164.506(a) that provides regulatory permission for covered entities to use or disclose protected health information for treatment, payment, and health care operations. A new provision is added at § 164.506(b) that permits covered entities to obtain consent if they choose to, and makes clear any such consent process does not override or alter the authorization requirements in § 164.508. Section 164.506(b) includes a small change from the proposed version to make it clearer that authorizations are still required by referring directly to authorizations under § 164.508.

Additionally, this final Rule includes a number of conforming modifications, identical to those proposed in the NPRM, to accommodate the new approach. The most substantive corresponding changes are at §§ 164.502 and 164.532. Section 164.502(a)(1) provides a list of the permissible uses and disclosures of protected health information, and refers to the corresponding section of the Privacy Rule for the detailed requirements. The provisions at §§ 164.502(a)(1)(ii) and (iii) that address uses and disclosures of protected health information for treatment, payment, and health care operations are collapsed into a single provision, and the language is modified to eliminate the consent requirement.

The references in § 164.532 to § 164.506 and to consent, authorization, or other express legal permission obtained for uses and disclosures of protected health information for treatment, payment, and health care operations prior to the compliance date of the Privacy Rule are deleted. The proposal to permit a covered entity to use or disclose protected health information for these purposes without consent or authorization would apply to any protected health information held by a covered entity whether created or received before or after the compliance date. Therefore, transition provisions are not necessary.

This final Rule also includes conforming changes to the definition of "more stringent" in § 160.202; the text of § 164.500(b)(1)(v), §§ 164.508(a)(2)(i) and (b)(3)(i), and § 164.520(b)(1)(ii)(B); the introductory text of §§ 164.510 and 164.512, and the title of § 164.512 to eliminate references to required consent.

Response to Other Public Comments

Comment: There were three categories of commenters with respect to the Rule's general approach to consent—those that supported the changes proposed in the NPRM provisions, those that requested targeted changes to the consent requirement, and those that requested that the consent requirement be strengthened.

Many commenters supported the NPRM approach to consent, making consent to use or disclose protected health information for treatment, payment, and health care operations voluntary for all covered entities. These commenters said that this approach provided flexibility for covered entities to address consent in a way that is consistent with their practices. These commenters also stated that the NPRM approach assured that the Privacy Rule would not interfere with or delay necessary treatment.

Those that advocated retaining a consent requirement stated that the NPRM approach would undermine trust in the health care system and that requiring consent before using or disclosing protected health information shows respect for the patient's autonomy, underscores the need to inform the patient of the risks and benefits of sharing protected health information, and makes it possible for the patient to make an informed decision. Many of these commenters suggested that the consent requirement be retained and that the problems raised by consent be addressed through targeted changes or guidance for each issue.

Some suggestions targeted to specific problems were: (1) Fix the problems

(3) That designates health care components in accordance with paragraph (c)(3)(iii) of this section.

* * * * *

(c)(1) *Implementation specification: Application of other provisions.* * * *

(ii) A reference in such provision to a "health plan," "covered health care provider," or "health care clearinghouse" refers to a health care component of the covered entity if such health care component performs the functions of a health plan, health care provider, or health care clearinghouse, as applicable; and

* * * * *

(2) *Implementation specifications: Safeguard requirements.* * * *

(ii) A component that is described by paragraph (c)(3)(iii)(B) of this section does not use or disclose protected health information that it creates or receives from or on behalf of the health care component in a way prohibited by this subpart; and

* * * * *

(3) *Implementation specifications: Responsibilities of the covered entity.* * * *

(iii) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation as required by § 164.530(j), provided that, if the covered entity designates a health care component or components, it must include any component that would meet the definition of covered entity if it were a separate legal entity. Health care component(s) also may include a component only to the extent that it performs:

(A) Covered functions; or

(B) Activities that would make such component a business associate of a component that performs covered functions if the two components were separate legal entities.

* * * * *

(f)(1) *Standard: Requirements for group health plans.* (i) Except as provided under paragraph (f)(1)(ii) or (iii) of this section or as otherwise authorized under § 164.508, a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the requirements of this subpart.

* * * * *

(iii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose to the plan sponsor information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

* * * * *

7. Revise § 164.506 to read as follows:

§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.

(a) *Standard: Permitted uses and disclosures.* Except with respect to uses or disclosures that require an authorization under § 164.508(a)(2) and (3), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart.

(b) *Standard: Consent for uses and disclosures permitted.* (1) A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations.

(2) Consent, under paragraph (b) of this section, shall not be effective to permit a use or disclosure of protected health information when an authorization, under § 164.508, is required or when another condition must be met for such use or disclosure to be permissible under this subpart.

(c) *Implementation specifications: Treatment, payment, or health care operations.*

(1) A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations.

(2) A covered entity may disclose protected health information for treatment activities of a health care provider.

(3) A covered entity may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information.

(4) A covered entity may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is:

(i) For a purpose listed in paragraph (1) or (2) of the definition of health care operations; or

(ii) For the purpose of health care fraud and abuse detection or compliance.

(5) A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to another covered entity that participates in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

8. Revise § 164.508 to read as follows:

§ 164.508 Uses and disclosures for which an authorization is required.

(a) *Standard: authorizations for uses and disclosures.*—(1) *Authorization required: general rule.* Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.

(2) *Authorization required: psychotherapy notes.* Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:

(i) To carry out the following treatment, payment, or health care operations:

(A) Use by the originator of the psychotherapy notes for treatment;

(B) Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or

(C) Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and

(ii) A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a); § 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; § 164.512(g)(1); or § 164.512(j)(1)(i).

(3) *Authorization required: Marketing.* (i) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of protected health

related to filling prescriptions by treating pharmacists as providers with indirect treatment relationships or by deeming a prescription to serve as an implied consent; and (2) allow certain uses and disclosures prior to first patient encounter. Some of these commenters argued that certain issues could be addressed through guidance on other provisions in the Rule, rather than a change in the regulation. For example, they suggested that guidance could explain that physicians who take phone calls for one another are part of an organized health care arrangement, or could provide technical assistance about revocations on consent by identifying when a covered entity has taken action in reliance on a consent.

Other suggestions were more general. They included suggestions that the Department: (1) Substitute a good faith effort requirement for the current provisions; (2) provide regulatory permission for certain uses and disclosures of protected heath information prior to first service delivery; (3) permit oral consent with documentation; (4) retain a consent requirement for disclosures, but not uses; (5) retain a consent requirement for payment and operations, but not treatment uses and disclosures; (6) allow individuals to opt out of the consent requirement; (7) allow the consent to apply to activities of referred-to providers, and (8) retain the consent requirement but add flexibility, not exceptions.

The third group of commenters requested that the consent requirement be strengthened. Some requested that the Privacy Rule not permit conditioning of treatment or enrollment on consent for multiple uses and disclosures. Others requested that the consent requirement be extended to covered entities other than providers with direct treatment relationships, such as health plans. Some commenters also asked that the consent be time-limited or be required more frequently, such as at each service delivery.

Response: The Department recognizes that there are some benefits to the consent requirement and has considered all options to preserve the consent requirement while fixing the problems it raises. After examining each of these options, we do not believe that any would address all of the issues that were brought to the Department's attention during the comment process or would be the best approach for regulating this area. For example, the suggestion to treat pharmacists as indirect treatment providers would not be consistent with the current regulatory definition of that term and would not have addressed other referral situations. This approach was also rejected by some pharmacists who view themselves as providing treatment directly to individuals. The suggestion to allow certain uses and disclosures prior to first patient encounter would not address concerns of tracking consents, use of historical data for quality purposes, or the concerns of emergency treatment providers.

The Department desired a global approach to resolving the problems raised by the prior consent requirement, so as not to add additional complexity to the Privacy Rule or apply different standards to different types of direct treatment providers. This approach is consistent with the basic goal of the Rule to provide flexibility as necessary for the standards to work for all sectors of the health care industry.

More global approaches suggested were carefully considered, but each had some flaw or failed to address all of the treatment-related concerns brought to our attention. For example, those who suggested that the Rule be modified to require a good faith effort to obtain consent at first service delivery failed to explain how that approach would provide additional protection than the approach we proposed. The Department also decided against eliminating the consent requirement only for uses and disclosures for treatment, or only for uses of protected health information but not for disclosures, because these options fall short of addressing all of the problems raised. Scheduling appointments and surgeries, and conducting many pre-admission activities, are health care operations activities, not treatment. Retaining the consent requirement for payment would be problematic because, in cases where a provider, such as a pharmacist or hospital, engages in a payment activity prior to face-to-face contact with the individual, it would prohibit the provider from contacting insurance companies to obtain pre-certification or to verify coverage.

Similarly, the suggestion to limit the prior consent requirement to disclosures and not to uses would not have addressed all of the problems raised by the consent requirements. Many of the basic activities that occur before the initial face-to-face meeting between a provider and an individual involve disclosures as well as uses. Like the previous approach, this approach also would prohibit pharmacists and hospitals from contacting insurance companies to obtain pre-certification or verify coverage if they did not have the individual's prior consent to disclose the protected health information for payment. It also would prohibit a provider from contacting another provider to ask questions about the medical record and discuss the patient's condition, because this would be a disclosure and would require consent.

There was a substantial amount of support from commenters for the approach taken in the NPRM. The Department continues to believe that this approach makes the most sense and meets the goals of not interfering with access to quality health care and of providing a single standard that works for the entire health care industry. Therefore, the Department has adopted the approach proposed in the NPRM.

Comment: Some commenters asserted that eliminating the consent requirement would be a departure from current medical ethical standards that protect patient confidentiality and common law and State law remedies for breach of confidentiality that generally require or support patient consent prior to disclosing patient information for any reason. Another commenter was concerned that the removal of the consent requirement from the Privacy Rule will become the de facto industry standard and supplant professional ethical duties to obtain consent for the use of protected health information.

Response: The Privacy Rule provides a floor of privacy protection. State laws that are more stringent remain in force. In order not to interfere with such laws and ethical standards, this Rule permits covered entities to obtain consent. Nor is the Privacy Rule intended to serve as a "best practices" standard. Thus, professional standards that are more protective of privacy retain their vitality.

Comment: Some commenters requested that, if the Department adopts the NPRM approach to eliminate the consent requirement for uses and disclosures of protected health information for treatment, payment, or health care operations, the definition of "health care operations" should also be narrowed to protect individual expectations of privacy.

Response: We disagree. As stated in the preamble to the December 2000 Privacy Rule, the Department believes that narrowing the definition of "health care operations" will place serious burdens on covered entities and impair their ability to conduct legitimate business and management functions.

Comment: Some commenters requested that the regulation text state more specifically that a voluntary consent cannot substitute for an authorization when an authorization is otherwise required under the Privacy Rule.

TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS
45 C.F.R. 164.501

"Treatment"

1. provision of health care
2. management of health care
3. coordination of health care
4. management of health care
5. consultation between health care providers relating to a patient
6. the referral of a patient for health care from one provider to another. 45 CFR 164.501

"Payment"

Activities by a health plan or a provider with respect to providing or obtaining reimbursement for services "including, but not limited to"

1. determinations of eligibility
2. determinations of coverage
3. adjudications of health claims
4. subrogation of health claims
5. risking adjusting amounts due based on enrollee status and demographic characteristics
6. billing
7. claims management
8. collection activities
9. obtaining payment under a contract for reinsurance
10. related health care data processing
11. review of health services with respect to medical necessity
12. review of health services with respect to coverage under a health plan
13. review of health services with respect to appropriateness of care
14. review of health services with respect to justification of charges
15. utilization review activities
16. concurrent review of services
17. retrospective review of services
18. disclosure to consumer reporting agencies

"Health Care Operations"

1. conducting quality assessment and improvement activities
2. development of clinical guidelines
3. population based activities related to improving health
4. population based activities related to reducing health care costs
5. population based activities related to protocol development
6. population based activities related to case management and care coordination
7. contacting of health care providers with information about treatment alternatives
8. contacting of patients with information about treatment alternatives
9. related functions that do not include treatment
10. reviewing the competence of health care professionals
11. reviewing the qualifications of health care professionals
12. evaluating practitioner performance
13. evaluating provider performance
14. evaluating health plan performance
15. conducting training programs for students, trainees or practitioners
16. training of non-health care professionals
17. accreditation
18. certification
19. licensing
20. credentialing activities
21. underwriting
22. premium rating
23. other activities relating to the creation, renewal or replacement of a contract of health insurance
24. ceding a contract for reinsurance
25. securing a contract for reinsurance
26. placing a contract for reinsurance
27. conducting or arranging medical review
28. conducting or arranging legal services
29. conducting or arranging auditing functions
30. conducting or arranging for fraud and abuse detection programs
31. conducting or arranging for compliance programs
32. business planning
33. business development
34. business management
35. general administrative activities of the entity
36. customer service including provision of data analysis for policy
37. resolution of internal grievances
38. sale of the covered entity
39. transfer of the covered entity
40. merger of the covered entity
41. consolidation of the covered entity
42. due diligence pertaining to items 38-41
43. creating de-identified health information
44. creating a limited data set
45. fundraising

"Treatment and payment" uses relate to providing health care to the individual while **"health care operations"** uses relate to operations of the covered entity. 65 Fed. Reg. at 82,489/3, 82,495/1, 82,4973.

MR. DEAL. Thank you. Dr. Detmer.

MR. DETMER. Good afternoon, Chairman Deal, members of the Health Subcommittee. I am Don Detmer, President and CEO of the

American Medical Informatics Association, whose 3,500 members include physicians, nurses, other health professionals, computer and information scientists and managers, biomedical engineers, academic researchers, and educators. Over the years AMIA's members have been the pioneers of information knowledge relating to healthcare. In the early days of HIPAA rulemaking from 1996 to 1998, I served as the Chairman of the National Committee on Vital and Health Statistics, and I also was a member of the IOM committees that produced the Errors report and the Chasm report. More recently, I was one of the Speakers appointments to the Commission on Systemic Interoperability.

It is a pleasure to appear before you today. I would like to briefly summarize a few key points, and my written testimony expands on those to some extent. The need for Federal leadership. Today, too few individuals have access to electronic health record systems and there is little interconnectedness of the systems that exist. And yet, significant improvements in healthcare safety and quality cannot be achieved without robust secure electronic record systems that can be securely communicated across a national information network as we heard from Mr. Neaman. Without Federal leadership our national goal of safe, efficient, effective, equitable, timely, and patient-centered care will remain unfulfilled dream because the necessary integrated health information systems will not be there.

My comments will touch on a few points that are needed to move our national vision forward at this time. First, the Office of the National Coordinator for Health Information Technology, ONC, led by Dr. David Brailer, is doing an excellent job. H.R. 4157, the Health Information Technology Promotion Act would establish the ONC in statute and AMIA applauds this. Second, the Department of Health and Human Services should be given explicit responsibility and sufficient ongoing resources for the National Library of Medicine to assure that the ongoing maintenance and open dissemination of agreed health information standards can be pursued as Dr. Braithwaite mentioned.

Similarly, we are pleased that H.R. 4157 provides explicit and reasonable rulemaking procedures for the Department to undertake long overdue upgrades of data vocabularies and classification systems, the U.S. thus showing the world and shaping global vocabularies and classifications as a source of primary data in electronic health records, including contemporary disease classifications and coding systems, specifically ICD-10, for a host of legitimate purposes that go well beyond reimbursement. Today they just do not accurately reflect modern medical practice, nor do they help the needs of medical researchers.

HIPAA. From my perspective as a physician, the privacy rule has been largely successful in clarifying the individual rights of all patients

in relation to their health data on a national basis in establishing the responsibilities and legal obligations of all providers to whom patients interact. It is now time to take a rigorous look at lessons learned. Some argue that States must have the capacity to enact more stringent requirements for privacy. In the name of better health and healthcare, I must respectfully disagree. In fact, I do not see how, in practical terms, we can get to widespread adoption of electronic health records without establishing meaningful floor to ceiling standards that preempt idiosyncratic State approaches. Speaking realistically, only through Federal and State leadership can we truly connect our Nation for healthcare purposes.

As a matter of record, AMIA has supported the need for appropriate Federal protection of genetic data. H.R. 4157 calls for a study of the impact of varying State statutes on the rights and protections afforded to patients and importantly on the impact of the requirements on the quality, cost, and effectiveness of healthcare. The study of HIPAA privacy and security standards represents an absolute minimum. Two other items will be valuable to add to the study. First, in addition to the effects on care, the study should examine effects on legitimate biomedical research. And, second, our Nation genuinely needs a consistent way to reliably and accurately authenticate the identity. Both safety and privacy are compromised when the right health information for one patient gets associated with or sent to the wrong patient.

Addressing disincentives to HIT dissemination. Reasonable safe harbors to permit dissemination of health information technologies and services intended to improve healthcare quality, efficiency, and access would encourage the deployment of essential health information systems. And I am very pleased that provisions to that effect are included in Chairman Deal's bill.

Educating the workforce. Ultimately health IT comes down to healthcare workers and patients being sufficiently skilled to take real advantages of the opportunities for improved care, efficiency, and access that health information technologies and the interconnected national health information infrastructure can provide.

In November 2005, AHIMA, the American Health Information Management Association, and AMIA, my organization, convened a workforce summit to develop initial strategies to address challenges relating to effective implementation of electronic health records and personal health records. The resulting white paper, I guess you might call it line paper, Building the Workforce for Health Information Transformation, presents nine targeted recommendations that key stakeholders, including government, can use to support the existing workforce and ensure that sufficient number of well-qualified health

information specialists are available to achieve the necessary health transformation through IT.

We commend this report to you, and AMIA and AHIMA stand ready to help address this challenge. I firmly believe that the development and deployment of an interoperable, interconnected national health information system is not purely a healthcare issue. It is a matter of national security. Whether we face, God forbid, another Hurricane Katrina or an outbreak of avian flu in humans or another episode of bioterrorism, we simply must have a reliable health information and communication system for our people's well-being. Our Nation's safety depends on it. Thank you again for the opportunity to testify, and I look forward to responding to questions.

[The prepared statement of Don E. Detmer follows:]

PREPARED STATEMENT OF DR. DON E. DETMER, PRESIDENT AND CHIEF EXECUTIVE OFFICER, AMERICAN MEDICAL INFORMATICS ASSOCIATION

Good morning. Chairman Deal, Ranking Member Brown, members of the Health subcommittee: thank you for the opportunity to appear before you today. My name is Don Detmer. I am President and CEO of the American Medical Informatics Association, whose 3200 members include physicians, nurses, computer and information scientists and managers, biomedical engineers, academic researchers and educators. Over the years AMIA has provided many of the thought leaders who have pioneered the innovative use of information technologies in healthcare. In addition to my role with AMIA, I am a Professor of Medical Education in the Department of Public Health Sciences at the University of Virginia. I practiced as a vascular surgeon for twenty-five years.

From 1996 to 1998 I had the privilege of serving as Chairman of the National Committee on Vital and Health Statistics, whose mission, broadly, is to advise the Department of Health and Human Services on shaping a national information strategy to improve the nation's health. My tenure at NCVHS coincided with the expansion of the Committee's charge enacted in the Health Insurance Portability and Accountability Act of 1996, which gave the Committee significant responsibilities in regard to administrative simplification and privacy. More recently, I was a member of the Commission on Systemic Interoperability, which was created by the Medicare Modernization Act, and which made a series of recommendations concerning the adoption and implementation of health information technology in an October 2005 report to Congress entitled, *Ending the Document Game: Connecting and Transforming Your Healthcare Through Information Technology*.

As you consider, and I hope pass, legislation that aims to facilitate movement toward a 'smarter' health care system through the promotion of widespread adoption of electronic health records (EHRs) and personal health records (PHRs), let me comment today on three important issues:

- first, there is a critical need for ongoing Federal leadership in encouraging and shaping a national health information system that benefits all stakeholders, especially patients;
- second, we should focus on "lessons learned" from the rollout of HIPAA standards to date and identify issues to be considered as additional health information standards and initiatives are developed and disseminated;

- and, third, we should address some current disincentives – both real and perceived – that slow the implementation of health information technologies in our healthcare system, the most information-intensive enterprise in our economy.

The Continuing Need for Federal Leadership

While it is the undoubted world leader in high technology clinical care and biomedical research, the US healthcare system is an incredibly fragmented mix of very large and very small players – a conglomeration of 21st century medical science and cottage-industry business practices, and too often characterized by uneven access, delivery and outcomes. Significant improvements in healthcare safety and quality will not be achieved for Americans without robust, secure electronic health records within a national health information infrastructure (NHII). Market forces alone have not driven the necessary integration of the interests and needs of disparate participants: hospitals – physicians and other providers – payers – employers – researchers – educators – and, most important, patients. As a result, too few individuals have access to electronic health record systems today and there is little interconnectedness of the systems that exist. Without Federal leadership to encourage the deployment of interconnected, interoperable health information systems, our progress toward integrated and quality-based care delivery will continue to be lurching and inconsistent.

AMIA has been encouraged by Congressional attention to health information issues as evidenced by the introduction of HR 4157, the Health Information Technology Promotion Act, and HR 2234, the 21st Century Health Information Act, as well as the passage by the Senate late last year of S 1418, the Wired for Health Care Quality Act. And, we have been pleased to provide input to several legislative proposals to make personal health records (PHRs) available to Federal Employee Health Benefit Plan (FEHBP) beneficiaries. These bills are important not only for their specific provisions, some of which I will focus on today, but also because they convey an important message to the public – that their elected representatives recognize the critical importance of improving the health care system in ways that will empower consumers, while also improving the quality, safety, cost-effectiveness and accessibility of healthcare.

Over the last two plus years, the Office of the National Coordinator for Health Information Technology (ONC), which is headed by Dr. David Brailer, a Fellow of AMIA's College of Medical Informatics, has done an excellent job in communicating a vision to support widespread adoption of interoperable electronic health records within the next 10 years. AMIA is pleased that among the projects currently funded by the ONC are contracts for an Internet-based national health information network and for the development of processes for the harmonization of the various health information standards that are emerging. AMIA itself has a contract with the ONC to create a plan for a national framework for clinical decision support. In regard to interoperability standards and the development of processes to certify health information technologies that can actually 'talk' to each other and will allow the seamless integration of information systems to facilitate quality care, AMIA is also very supportive of the work of the public-private American Health Information Community (AHIC).

We believe strongly that HHS should be given explicit responsibility for ensuring the ongoing maintenance and dissemination of health information standards, with authorization for licensing and/or other types of support. To give you a successful example of Federal leadership, I would point to Secretary Tommy Thompson's drive to complete the licensure and distribution of SNOMED-CT, a vital 'dictionary' of medical terminology, by the National Library of Medicine in 2004. AMIA firmly believes that the Department should draw heavily on the resources and expertise of the NLM, and we support additional funding for the Library to ensure that approved vocabulary and other data content standards are maintained, coordinated and updated regularly to permit

appropriate alignment and uniformity of the sets of standards that underlie genuinely workable EHRs and PHRs. Just like the NLM's PubMed, these standards should be openly available on the internet.

Importantly, HR 4157, the Health Information Technology Promotion Act, introduced by Chairman Deal and Representative Nancy Johnson, provides explicit and reasonable rulemaking procedures by which HHS can undertake long overdue upgrades to data vocabularies and classification systems. Simply, if we are going to facilitate development of an interoperative nationwide network of electronic health records (EHRs), we must address the issue of interoperative data. This means that we must have standard vocabularies as the source of our primary data in the electronic health record, and use contemporary disease classifications and coding systems, (ICD-10), not only for traditional reimbursement purposes but to permit meaningful and accurate secondary uses of data for quality, biosurveillance, and public health monitoring, health research, injury prevention and policy making. As a physician and a health informatician, I find it unacceptable that the US remains one of a true handful of countries in the world to use a 30-year old classification system for diagnoses and inpatient procedures. If we are serious about deploying electronic health record systems for the benefit of individual patients and the nation as a whole, we must attend to the need to improve data standards and speed our capacity to update those standards. At the end of the day, our data systems and standards should primarily foster better care, not better reimbursement.

HR 4157 establishes the Office of the National Coordinator for Health Information Technology in statute, and I believe this step is a crucial one in clarifying Federal leadership. As part of our support for the Office of the National Coordinator, AMIA will continue to urge the appropriators on both sides of the Hill to provide for adequate funding of the ONC.

Examining HIPAA Lessons Learned So Far

As we move to develop an interconnected, interoperable health information system that will facilitate quality, access and patient-centeredness on a national and international basis, it is prudent to identify lessons we have learned so far from the administrative simplification provisions of HIPAA. Though the road was often difficult, if not actually painful, we have made a great deal of progress in establishing the rights of individuals to expect that their health information will be used appropriately and their privacy and confidentiality protected, and in imposing meaningful and reasonable obligations on health care providers, plans and payers, and others to comply with consistent Federal standards for the use, disclosure and transmission of health information.

Where once some people in the healthcare system may have treated individual health information too cavalierly on at least some occasions, from my perspective it is manifestly clear that since the Privacy Rule took effect in 2003, doctors, hospitals, pharmacies, health plans and others have made really extraordinary efforts to inform individuals of their rights and to establish policies and procedures that protect sensitive health information. Today every individual has a Federal right to access his or her medical record and to expect that the healthcare system will keep that record secure and confidential. And these norms are national – no longer are your rights, or the legal responsibilities of those healthcare providers you deal with, defined by the unique features of the State in which you live. Even if HIPAA may have 'backed' the nation into reasonable privacy and confidentiality protections, the roll-out has proved, on the whole, successful.

Notwithstanding what I think have been extremely good faith efforts to ensure that personal data is adequately protected, I do not discount that some people – for instance, those with concerns about the security of especially sensitive information, such as HIV status or relating to mental health treatment – have continued concerns about health privacy. To my knowledge there have not been reports of any large-scale violations of

the framework set in place by the HIPAA Privacy Rule. That is, individually identifiable health information is used and disclosed only for "treatment, payment and health care operations" or as otherwise specifically authorized by the individual. Does the Privacy Rule protect against patently unethical or extraordinarily careless acts – like the leaking of a celebrity's medical record to a tabloid magazine or the disposal of old medical records in a dumpster or a straightforward instance of identity theft? Of course not – but we cannot expect even the most carefully crafted information standards to prevent all illegal behavior. In such instances, active pursuit and strong penalties are needed when intrusions and misuses are identified, as a lesson to dissuade others from similar illegal behavior.

Some argue that the States must have the capacity to enact 'more stringent' standards for health information – as is true under the current Privacy Rule – for all health information standards, including those that are absolutely necessary for the development of an interconnected, interoperable national health information system. In the name of better healthcare, I must respectfully disagree. About half of all Americans live near State lines and multiple State approaches complicate the efficient and seamless transmission of crucial health information. For example, it is hardly unusual for an individual to work in the District, live in Maryland, and receive health care in Virginia, with payments made by an insurer located in still another state. If we are to ensure real-time availability of accurate and complete clinical information at the point of care, we simply cannot have the standards for the use, disclosure and transmission of the patient's health information subject to idiosyncratic requirements of individual States.

Personally, I don't see how we can get to the common standards and interoperability that underlie the widespread adoption of electronic health records without Federal preemption of conflicting State laws. But rather than simply assert that proposition, let me note that, in relation to the Privacy Rule, since 1999 AMIA has called for a study of the impact of the lack of Federal preemption and the impact of varying State statutes on the rights and protections afforded to individuals <u>and</u> upon the quality, cost and effectiveness of health care. Thus, I am very pleased that HR 4157 calls upon the Secretary to undertake such a study in relation to standards that have been adopted subsequent to HIPAA. This is a prudent approach; however, if the study shows that varying State laws and requirements have a negative impact on health care delivery, quality and access, and that HIPAA has established meaningful privacy and security protections, it makes sense to move forward without delay on Federal preemption for all adopted HIPAA standards.

As you may recall, the original HIPAA legislation called for the development of a unique personal healthcare identifier for individuals. All other developed economies in the world have already or are currently implementing such identifiers to assure proper authentication of people seeking care services. Whether we do so with via a voluntary opt-out approach or through the use of reliable identification algorithms, the United States needs a uniform approach to authenticating one's identity, and having the benefit of a unique identifier to help increase the ease and accuracy of this authentication is not trivial. Indeed, I fear that short of such a move, we will be left behind the other nations with whom we should be seeking secure ways to collaborate on global standards. This topic was a key recommendation from the Commission on Systemic Interoperability, and I would strongly recommend that consideration of the issues involved in the reliable authentication of individuals be included in the Secretarial study called for in HR 4157.

<u>Disincentives That Have Slowed Implementation of Information Technologies</u>

From 1999 through 2003 I had the privilege to serve as the Gillings Professor of Health Management at Cambridge University in England and to consult to the National IT programme of the National Health Service. As you may know, the British government is investing billions of pounds to implement a fully functional, patient-friendly, electronic

health record and system. While this task might appear to be easier in some aspects because of Britain's single-payer system, of particular note to me was the observation that, even before the government's new investment, well over 80 percent of England's primary care physicians were facilitating patient care electronically. Today they are moving forward with booking appointments, writing prescriptions, making electronic referrals, recording clinical notes and tracking treatment compliance. By contrast, it is estimated that fewer than 20 percent of US primary care physicians utilize electronic health records.

Interestingly, England's primary care practices were 'wired' initially not because of government investment, but because the British pharmaceutical industry years ago offered to supply the necessary hardware and software to primary care doctors in return for access to anonymized prescribing information. In the United States I think such an arrangement would be seen as unseemly at best, and illegal at worst; certainly in the U.K. there were those who held the same view. While the British are neither less ethical nor more permissive of the misuse of identifiable health information than are Americans, in this country hospitals, physicians and other providers are incredibly reluctant to pursue any innovative financing for health IT, including networks that can securely link together a region's providers, because of their concerns about the Stark self-referral prohibitions and other fraud and abuse standards.

Whether these concerns are reasonable, today we have hospital lawyers who absolutely insist that it is simply not acceptable for any third party to furnish any information technologies – whether hardware, software, training or other services – to any provider at less than a full, fair market price. Yet, the aims of HIT dissemination are to improve the availability of accurate and timely health information in order to improve the quality of care, and I am aware of no evidence that such dissemination by a hospital, for instance, could actually serve to drive 'new' referrals or business into that hospital. While some healthcare systems and providers are moving forward under the current standards, the general consensus in the healthcare community is that the Stark provisions, while quite important in many respects, are significantly constraining progress on the roll-out of electronic health record systems.

It is in the interest of all stakeholders, particularly patients, that functional electronic health records and an interoperable health information system be deployed as promptly as possible. But the entities that are one key to making crucial progress with that deployment, the small and rural physician practices that still provide a majority of health care services in this country, are those that are least able to afford the capital investment for the purchase and hassle of implementing state-of-the art IT systems. Especially because most of the 'savings' of health IT accrue to other system participants, including employers, health plans and patients, financial outlays necessary for the purchase of the very building blocks of an NHII should reasonably come from a wide variety of sources, including government outlays and pay-for-performance programs. Actually, pay-for-performance programs represent a clear argument for payers to provide some of the financing for health IT – because in order to pay-for-performance you have to be able to track performance and quality in the delivery of care, and to do that efficiently you need sophisticated information capabilities embedded in the healthcare system. Reasonable safe harbors for dissemination of health information technologies and services intended to improve healthcare quality, efficiency and access would encourage deployment of essential health information systems, and I am very pleased that provisions to that effect are included in Chairman Deal's bill.

Educating the Healthcare Workforce

There is no question that momentum for bringing healthcare into the information century is building, but this won't happen purely through a widespread distribution of hardware and software and standards and certifications. Ultimately, IT comes down to

healthcare workers and patients being sufficiently skilled to take real advantage of the opportunities for improved care and efficiency and access that health information technologies and an interconnected national health information infrastructure can provide. Assuring these skills throughout the workforce will necessitate sufficient numbers of well educated health informaticians. Because the field is advancing so rapidly, we are seriously undersupplied to meet this challenge.

Last year to help address this challenge, AMIA announced its 10 by 10 program, which aims to realize a goal of training 10,000 health care professionals, especially in applied clinical informatics by the year 2010; we just passed our first 100 graduates of a largely web-based course developed by William Hersh and his colleagues at the Oregon Health and Science University. Other universities intend to participate as well. Our program uses classes, tutorials, web-based and in-person sessions to equip health care professionals to use health information and health information technologies to benefit patient care and to advance medical knowledge. In fact, we know from the research of AMIA members that well-trained health providers combined with robust IT systems can produce safer, higher quality care delivery.

With the supply of physicians essentially constant and the nursing workforce aging along with the baby boomers, we will only be able to address the increasing demands for care of a growing and aging population by developing a better trained workforce, especially more nurses skilled in the use of information and information systems. Increased Federal support for education and training will be needed to address this workforce reality – and in November 2005 AMIA, in conjunction with our colleagues of the American Health Information Management Association (AHIMA), convened a workforce summit, which included broad representation of stakeholders across the healthcare enterprise, to develop initial strategies to address challenges related to effective implementation of EHRs and PHRs. The resulting white paper, *Building the Workforce for Health Information Transformation* presents nine targeted recommendations that the industry – including employers, employees, vendors, the government and professional organizations – can use to prepare the existing workforce to use technology tools and to ensure that we have a sufficient number of well-qualified health information specialists to achieve the promise of health IT transformation.

A Few Conclusions

In terms of the development and implementation of integrated health information systems with sophisticated capabilities, we have seen a great deal of progress in the last few years. Within the Veteran's Administration, for instance, the case for improved safety and higher quality through the proper use of IT systems – including electronic records, decision-support programs, and process tracking and change analyses – has been largely made. We have seen the creation of the Office of the National Coordinator for Information Technology and a Commission to Certify Health Information Technology. The Commission on Systemic Interoperability mandated by the MMA has provided an important set of recommendations to Congress, and Secretary Leavitt has pressed the American Health Information Community (AHIC) to take on a range of public-private initiatives to develop information standards, certify new technologies, and provide long-term planning and governance for the electronic health environment.

Someday we may look back at this moment and say, "The rest is history" – but not just yet. Additional legislation and Federal support, and the development of accepted, enterprise-wide standards will be required if true interoperability and connectedness are to occur. Clearly, HR 4157 does not try to address all of the issues involved in creating an NHII to improve healthcare quality, access and patient-centeredness. But it does forthrightly address some key 'sticking points' that are keeping the nation from moving forward as quickly as we should and among them are first, establishment of the Office of the National Coordinator in statute; second, addressing the impact on patient's rights and

on healthcare quality and safety of varying and conflicting State and Federal information standards; and, third, reducing some current disincentives to the adoption of available health information technologies. AMIA looks forward to prompt consideration of the legislation and to supporting its implementation.

Finally, let's not forget that an interoperable, interconnected national information system is not only a healthcare issue; it is a matter of national security. When I testified to the House Ways and Means Committee on July 25, 2005, I stated that it wasn't clear what would bring this reality to the American public. I mentioned an outbreak of avian flu in a US population center or an episode of bioterrorism or the occurrence of transmissible disease in our food supply chain. Instead, a few months later Hurricane Katrina drove home my point. In the first weeks and months after this national disaster, two contrasting points were made abundantly clear. First, public health and individual patient care of thousands of Americans was jeopardized as paper medical records were destroyed by mud. Second, the electronic medication and health records of veterans were available wherever and whenever their availability was authorized, offering immediate help to hundreds. People's lives do hang in this balance.

We must have a reliable, ubiquitous electronic health information system for our nation. It is crucial for personal health, public health and the economic interests of our country. While widespread dissemination of electronic health record systems and the development of a functional NHII will facilitate broad improvements in health care quality, access and affordability, it will also assist in protecting our security and I would urge your leadership in facilitating this development with all due speed.

Thank you for the opportunity to appear before you today. I will be happy to answer any questions.

MR. DEAL. Thank you very much. Thanks to all of you. There were some very interesting comments. I think with maybe one exception, Mr. Pyles being the exception, most of you have agreed we need to do something in this area. Mr. Vaughan has his reservations about it. I understand the privacy issue, and I certainly agree with it. Hearing some of the testimony sort of reminds me of the old joke about the fellow who went to his doctor, and the doctor asked him, what is wrong with you, and he says that is what I am paying you to figure out. We all want to protect our privacy but there has to be some degree of sharing of that. Now I think that the question of preemption of State law is one of the more significant issues that we have to deal with here.

I understand too that there are some very pragmatic problems when you allow States to have their own set of rules. My congressional district borders three States, and the Chattanooga area is to the immediate north of my district. We have doctors who have patients that go to the hospitals in Chattanooga. Other parts of my State, of course, Augusta, which is on the South Carolina border, Columbus, which is on the Alabama border, if we do not have some degree of uniformity of those kinds of regulations statutorily, how do we avoid, if nothing else, those cross-State dealings back and forth of the hospitals and doctors who may be in different States, how do we avoid those kind of problems where one State's rules may be different from the other State's rules? Is that a problem or is that not a problem? Mr. Pyles.

MR. PYLES. I would be glad to address that, and I also want to say that I do not disagree that something needs to be done in this area. I think something needs to be done particularly with respect to HIPAA because you have got HIPAA authorizing disclosure for treatment and payment of healthcare operations in your State and most others and standards of medical ethics prohibiting it, so it causes confusion in the consumer community. They do not know if they have a right to privacy or not, and this leads to confusion in the practitioner community. I think a good argument can be made for having greater uniformity and therefore understandability in the privacy standards across the country.

MR. DEAL. Should we not be able to all agree on what those would be?

MR. PYLES. I would agree with that, and that is why I cited the standards of medical ethics which apply across the country that contain a consistent privacy standard that has been applied for years, cited the constitutional common law that applies in every State, the psychotherapist-patient privilege, and the patient physician privilege which again applies under the State. What we are suggesting is let us look at the common standards we now have that apply across the country and all three of the States your district borders on. Every doctor in those States is subject to standards of medical ethics, everyone is subject to the constitutional common law and physician-patient privilege. We have national standards for privacy. We just do not have them in Federal law.

MR. DEAL. Mr. Vaughan, you made reference to a possible model law. Is there one that has been proposed by the National Association of State Legislators, for example?

MR. VAUGHAN. Not to my knowledge. I am just reading Don's testimony. This is a problem and how do we deal with it. And it strikes me that under your leadership you could call for the NGA and the National Conference of State Legislators to come together and to really identify where the differences are and where the commonality is, and like when you make a change in long-term care insurance you give the NAIC a couple years to come up with a model, Reagan stuff, and then it goes into effect. You could set up a structure that kind of brings the States together and say what is really important to us and let us try to talk a common language and not this tower of babble, and you have a couple years to do it.

It is such detailed work. You do not want this all on your desk, I would think. Get these groups together and see where the commonality lies, and let us try to bring this up for the American public rather than down to a minimum.

MR. DEAL. Mr. Mertz.

MR. MERTZ. Mr. Chairman, I just wanted to comment on that. We think that the HIPAA standard does create some uniformity. The weakness of it is that it does not preempt these literally thousands of conflicting State rules that are creating an obstacle. And the examples I gave you were various States that actually bar the laboratories from providing lab results. If you set up regional organizations or web-based electronic health records, under the State laws that exist today, we could not transmit laboratory results which make up 60 percent of someone's medical record. That medical record that is on the web would be missing 60 percent of the data that a physician needs. And so we think that the HIPAA standard is a very good one and very protective and sets the standard.

We believe that preemption is necessary. You are only doing a study which I think would hopefully identify these conflicting State laws to have the States go back and try to undo the laws. I was involved in doing a study of State laws. There are thousands and thousands and thousands of rules that would take 100 years for the States to unravel all of those. That is why we need one good strong Federal standard.

MR. DEAL. My time is expired. Mr. Waxman.

MR. WAXMAN. Thank you, Mr. Chairman. Following along the same inquiry, I am concerned about creating a national health information infrastructure without strong privacy protections for patients. HIT will allow providers to not only keep their patients' healthcare records electronically, but share them with others more easily. I do not presume that any of you would be comfortable letting an employer or a health plan know if you were genetically predisposed to mental illness or have the public know your grandchild had been exposed to AIDS or allow a co-worker to learn that your husband or wife has a fertility problem. These clearly are very private matters.

With the expansion of the use of electronic medical records comes an increase in the potential for breaches of privacy and the pirating of sensitive personal medical information by unauthorized parties. HIPAA, the Health Insurance Portability Accountability Act, set minimum Federal standards for use in disclosure of personal information. However, when HIPAA was passed, Congress was unable to come to agreement in certain areas so States were allowed to enact additional consumer protections. Similarly, Congress has been unable to come to agreement and pass a Federal genetic non-discrimination law prohibiting employers from learning about and using genetic information about their employees in the work place. Still, there are some HIT proponents who would be comfortable with HIPAA as a Federal privacy standard that would also preempt all State privacy and security laws such as State genetic non-discrimination laws. So Mr. Pyles, could you comment on

what would have to be included in a Federal privacy law for it to be protective, especially if it were to supersede State laws?

MR. PYLES. Thank you. I will be glad to do that. First and foremost, I think we would want to see a law grounded in the principles, as I said, of standards of medical ethics, otherwise, we would have Congress perhaps authorizing the unethical practice of medicine, which I do not think any physician would want to see happen or any practitioner. It ought to be granted, and the right to privacy reflected in our founding principles of the Constitution, and again those are remarkably similar. There was a comment about thousands of State laws. In fact, there are core concepts in those laws that are remarkably similar. As I said, every State protects mental health information, recognizes a psychotherapist-patient privilege, but beyond that we would need things that HIPAA does not provide. Things like breach notice requirements where patients whose privacy has been breached will be notified and the Secretary will be notified so that we can see a list of companies that do not do a very good job of protecting medical privacy. That could probably be the best enforcement measure we could have.

There should be a private right of action that nearly every State recognizes because we know that HHS has done a very poor job. There are over 17,000 privacy complaints that have been filed since April 14, 2003, the implementation date of HIPAA, and only one enforcement action. So we think that there should be an opportunity for patients to establish electronic black boxes. We do not think IT and privacy are incompatible. We think you can actually enhance privacy through the use of health IT, but you need to establish the principles at the beginning. You cannot retrofit an IT system for privacy.

MR. WAXMAN. Some States know the ways personal health information can be used without consent. Many States have more protective laws about specific types of sensitive information, HIV/AIDS, mental health records, genetic tests and more. And many States have more meaningful consent requirements. These are the kinds of things you think ought to be in a Federal law if we are going to have preemption.

MR. PYLES. I would agree. I would support perhaps a study done by the Secretary as H.R. 4157 provides. But it would have to be a study that is first and foremost directed to identify the commonalities that we see across the country in medical ethics and State laws, in constitutional law. We should build on the foundations we have and that we've formed in this country. We should not assume that we have to operate with a blank slate.

MR. WAXMAN. The Federal law only directly applies to providers, health plans, and health clearinghouses. Many States' privacy laws

directly apply to a broader range of individuals and entities like those that transcribe records or those that copy or transport files. Do you think that ought to be a Federal law?

MR. PYLES. Absolutely, Mr. Congressman. Oddly enough, HIPAA does not apply to hackers unless they happen to be providers or insurers or healthcare clearinghouses. We would think that as with many State laws, Congress should provide for privacy protections that run with the information and should apply to whoever handles the information. It is the same to the patient whether a private individual breaches their privacy or an insurer.

MR. WAXMAN. Thank you very much, Mr. Chairman.

MR. DEAL. Thank you. I hope we will have a second round too. If we do not have more Members show up, we may have a chance to go around again. Dr. Burgess.

MR. BURGESS. Thank you, Mr. Chairman. I forget who it was in their opening statement that referenced the disasters down on the Gulf Coast, which there is no place clearer that we do need to fix this problem. The records room at LSU, you walk through there, the place is ruined and will be ruined for the rest of our natural lifetimes. Contrast that with the parking lot at the arena at Dallas, Texas where you had 400 private doctors show up to triage people after they got off the buses from the Superdome. And I do not remember the drugstore precisely, I think it was Walgreen's, set up one of their remote computer terminals there. They did not have medical records, but at least they had pharmaceutical information on a lot of the people that got off the buses, and it made piecing together the medical story a lot more straightforward, so the value was proven to me that day, but it a difficult climb.

And, Mr. Nelson, I just wondered if you had a thought as to how much, looking forward, how much is this likely to cost? If we just look at the Federal government component of healthcare, Medicare, Medicaid, VA, Federal prison system, Indian Health Service, Federal qualified health centers, about 50 percent of the healthcare expenditures are accounted for by the Federal government. Do you have an idea as to what it is going to cost Secretary Levitt when he says he is going to build this platform?

MR. NELSON. I cannot give you a specific number. I can say that some of the building blocks that have been put in place, I think by Dr. Brailer if you take the proposal, for example, it essentially was a lot like what a venture capitalist would do when they are trying to infuse an investment and then get a return on that investment. Although that may have been about a $20 million investment on his part spread out across four major corporations, I could tell you for a company like IBM we are taking that and we are starting to build on it. At the end of the day, I

suspect that we will probably invest 10 to 20 times that amount into helping to fix the healthcare problems as a part of our replicating the opportunity that he has provided us across this country.

So, you know, I applaud that immensely without necessarily having a number that the actual Federal government itself has to invest. I think private enterprise is going to go a long ways in helping solve the problem.

MR. BURGESS. When I think back to my days in practice, it is a big expense for a single physician's office to do this. If a hospital puts in an expensive system they of course have borne the cost of that, then to bring individual doctors offices on board would be a relatively inexpensive process because most of the software expense has already been handled. But if the doctors offices then have to individually go out and contract with the software licenses and what have you it does become a good deal more expensive. So, Mr. Neaman, I wonder if there are any thoughts you have of how we might reform some of the Stark laws to allow this to be a more facile process.

MR. NEAMAN. Thank you. Your comments are absolutely on track in terms of the relative cost and the ability of extending from the hospital systems to doctor offices. In our own experience for our three hospitals, again we invested a little bit over $40 million to get the system up and running. In our experience it takes on an incremental basis of approximately $50,000 per physician to incrementally bring additional doctors up on the system, so it is a rather large expense. It is also a time consuming expense. We are inhibited by Stark and the anti-kickback provisions from extending our system to other physicians who are in independent or private practice, and that is a big hurdle to overcome, not a risk that we want to take given the penalties that are involved with those statutes. So it would be a relatively easy thing to extend the systems and the software to other physicians if we are permitted to do it under the Stark regulations.

MR. NELSON. If I could comment on that, please.

MR. BURGESS. Yes, please.

MR. NELSON. The $50,000 is certainly a substantial amount of money. To put that in perspective, our data shows that that will represent the cost. The actual market pricing and what physicians are willing to bear, the costs that they are actually willing to pay, is probably more than $300 to $400 per doctor per month range, so there is a bit of a gap there between what the cost is and what the delivery is. Of course, with the Internet and hosting services they do not necessarily have to go out and buy complete systems. The average size of a physician's group is like 2.5 or less, so they are small groups. They do not have the capital to be

able to spend the money, and so we are going to have to come up with alternate solutions that are very cost effective to make that work.

MR. MERTZ. Congressman, can I make a quick comment on that? We represent the labs and you were not in the room at the time.

MR. BURGESS. Let me make one other point because I am about to run out of time. If we get a second round, I will be happy to come back to you. From the physician's perspective too it is also a question of time for us to do electronic prescribing or even electronic medical records. The average physician has to see between 30 and 50 patients a day in order to pay the overhead and take something home, and if you add a minute and a half to two minutes to every transaction in order to be up to date with electronic medical records or prescribing that is two hours, and how are we going to compensate the physician for that time?

MR. NELSON. We are actually doing this right now in Westchester County up north of New York City. There are 60,000 IBM employees. The HR department of IBM actually provided an incentive to the physicians to the tune of 50 cents per member per month to actually use the system, so they get paid in order to get the cost benefits, and what not on a minimum level of adoption. The ROI on that was less than two years. We are seeing a much higher level of adoption than what we expected, you know, but it is a great model, I think, that we could use across other endeavors like this. And I agree 100 percent with your comments on time and doctors.

MR. BURGESS. But there the insurance plan bore some of that expense to incentivize the doctors to practice.

MR. NELSON. And we need to keep in mind that a great deal of benefit that comes from these systems goes back to the employer and to the payer.

MR. BURGESS. Sure. Thank you, Mr. Chairman.

MR. DEAL. Ms. Capps.

MS. CAPPS. Thank you, Mr. Chairman. I have about four or five questions I want to try to get into the brief time so I am maybe asking for brief responses. Mr. Nelson, I will start with you. We have been hearing from others on the panel about the complexity of multiple State privacy laws. I wanted to know technologically do we have--can you speak to the capability of technology to accommodate different State privacy laws?

MR. NELSON. I do not think it is a technical problem at all.

MS. CAPPS. Okay.

MR. NELSON. The technology can handle it and we have experience with ATMs, the banking industries, all of which have their own unique regulatory issues.

MS. CAPPS. So that is not the issue. But then let me ask about privacy, and I guess I will address you, Mr. Pyles, but I do not care who jumps in. Under current legislative proposals do patients have to consent to having anonymous information shared with researchers? Do they have to give their approval?

MR. PYLES. I am sorry. Could you restate the question?

MS. CAPPS. Under current legislative proposals, or at least some of them, do patients have to consent like give some significant assent either in writing to having anonymous information shared with researchers?

MR. PYLES. Well, I do not know about pending legislation. If it is de-identified information then it certainly could be disclosed under HIPAA.

MS. CAPPS. Without them even knowing if it is anonymous.

MR. PYLES. Without them knowing, that is correct. Yes. And under the proposed legislation, I cannot think of any of the proposed legislation that addresses that issue.

MS. CAPPS. The way it is now then, who is responsible for determining whether this is legitimate, you know, if lines have been crossed if there has been boundaries, and in proposed legislation?

MR. PYLES. Well, under HIPAA it is very, very difficult to know that their information has been disclosed and therefore, since they get no consent or opportunity, so that in effect is no notice, I am stunned that there are 17,000 complaints that HHS has received because I do not know how those patients would have known. So there must be many thousands, tens of thousands more breaches of privacy that are out there that people would object to if they just knew about it, but they probably do not.

MS. CAPPS. And they do not know about it. In some of the proposed legislation, is this dealt with?

MR. PYLES. No, that is one of the things most disturbing about all of the legislative proposals I see. It seems that privacy is always the last issue to be discussed, if it is discussed at all. A number of the proposals do not mention anything about privacy at all.

MS. CAPPS. They do not mention privacy at all.

MR. PYLES. Correct.

MS. CAPPS. Well, that is certainly something I would hope, given the questions today that certainly is on our minds, and we reflect our constituents so I am hopeful that this will be interjected into any kind of studies. Mr. Chairman, I would hope that that would be the case. I am wondering now with the little more time that I have if you, Mr. Pyles, or anyone could comment on some of the shortcomings in Federal law currently with regard to enforcement of Federal uses of personal health

information. You touched on it a bit. The disparity is, are there States that do a better job, for example?

MR. PYLES. Well, States can do a better job but even with the authorization for disclosures, without consent under HIPAA, it also means that patients often cannot even assert the rights they have under State law because many States prohibit the disclosure of many types of information. But HIPAA allows the disclosure, and if a practitioner follows HIPAA then not even a patient would know enough to assert their State rights. Plus HIPAA requires a notice of privacy practices to be given to every individual. The notice compels the practitioner to describe the disclosures that are made under HIPAA, authorized under HIPAA, even if that is not their practice.

So they are all supposed to include a notice of rights the patients would have under State laws, but I have seen very few notices that include any reference to State rights.

MS. CAPPS. But Mr. Nelson, if we can use him as the standard, says there is no barrier in the technology for allowing--

MR. PYLES. I have total confidence in Mr. Nelson. If Congress said that a national privacy standard had to reflect the right to privacy under medical ethics, constitutional law, and law of privilege, that tomorrow morning Mr. Nelson would have a product on the street that did just that, and also accounted for variations in the State laws.

MS. CAPPS. And accounting for the variations in State laws, so there is nothing that should stand in the way of this being pursued in the interest of consumers or patients.

MR. PYLES. Well, I am not the--

MR. MERTZ. Could I comment?

MS. CAPPS. I would love to hear--

MR. MERTZ. I am with American Clinical Labs. What is a technological barrier, the example I gave there is definitely a barrier in State laws. I gave the example of in Florida and Georgia, the laws do not allow the laboratories to transmit results to an electronic health record. If there is a disease management program that has been mandated under Medicare, we cannot transmit because they forbid us transmitting lab results to anybody except the ordering physician, even with the patient's consent. We cannot provide lab results for disease management, for an electronic health record.

So with all due respect, maybe you could build a computer that could do it but we cannot transmit the results, so that is a State barrier that is absolutely insurmountable for us with these programs.

MR. DEAL. That would be a very remarkable State law that did not allow a disclosure with patient consent.

MR. MERTZ. Well, it is not remarkable in Georgia and Florida.

MR. DEAL. Well, I know one thing. The citizens of Georgia care a lot about their privacy judging from the laws you have on the books.

MR. MERTZ. Well, it is not remarkable there because there are dozens of States that have those laws, so it is not unusual at all, Mr. Chairman.

MR. DETMER. I do think that one of the really strong points is that you do mandate a study and I think there will be things we will learn from that, and I think that is why in fact I really am so supportive of that part of the legislation.

MS. CAPPS. Mr. Chairman, this has been a good hearing.

MR. DEAL. Thank you very much. Mr. Green.

MR. GREEN. Thank you, Mr. Chairman. Having served years in the legislature before, I tell people I lost my mind and came to Congress. I am surprised a lot of States have it where they prohibit the individual patient from receiving that information. I assume it is not just Georgia and Florida. It must be a number of States.

MR. MERTZ. Well, it is unusual and it is one of those areas where the State law actually prohibits the patient from having access to their own records, which we find kind of odd. Again, we are the labs. We do the testing, and our business is really to get the data back to the physician. But, you know, Congressman, there are so many important things. Diabetes management, they need to get hemoglobin H1C tests every six months. We have almost 10,000 people die a year just because they are not tested for their hemoglobin regularly. So these programs are so important to save people's lives, or cholesterol, people with heart disease. It is essential that these programs be able to manage their disease, and so that is why, while we are very careful, we do not want to give results out to everybody. Genetic tests, we are the people who do the genetic tests. We certainly do not want to send those out to anybody who does not have an absolute need for disease management, hemoglobin, diabetes, asthma, heart disease, yes, those are important tests but we will be careful about it.

MR. GREEN. Mr. Vaughan, do you have a response to that?

MR. VAUGHAN. We are very much for consumers being able to have access to their medical records and if there is an error in there and it asks for an edit and a correction, yes, this is the kind of thing that we need to work out.

MR. GREEN. Can you tell me, does Texas have that prohibition?

MR. MERTZ. I have not looked at Texas specifically. I know that Georgia, Florida, New York, California do have them. I would have to get back to you on Texas.

MR. GREEN. We can check because--

MR. MERTZ. Generally what the State laws say is that the ordering physician or his or her designee may get the lab results, and unfortunately it has been interpreted to mean the designee is only someone in the doctor's office can get the results so generally, almost in every State, we cannot report to a RIO or to a disease management organization, so I think Texas would be the same.

MR. GREEN. I will have to talk to my legislators because that is a concern because I think the patient ought to make that decision anyway. Mr. Vaughan, you give some examples of your concern about the abuses under the Stark and anti-kickback laws, and Dr. Burgess talked about, and the panel all morning has talked about some of the things we have to do to be able to protect that. How are physicians' choices influencing the patients affected now on some of the examples?

MR. VAUGHAN. Well, the law was designed to deal with the fact, and started with labs, that doctors who invested in a lab everybody who walked in, you know, maybe just, gee, am I pregnant, would get a full lab workup. There was just documentation by GAO and OIG of tremendous over-utilization, and then we found the same things in X-rays and MRI machines and so forth, and so it spread to try to get a bright line because the anti-kickback laws, you have to prove intent. This was meant to be a bright line to say, gee, people who make these investments or get remuneration tend to, whether they are aware of it or not, start over-ordering and start doing more of a particular service, and it was driving up cost something awful.

The worry is that if stuff is provided free or at a reduced rate to a doctor it makes you a good friend of that person who gave it to you, and you tend to gravitate that way. Maybe that is not the best place to send your patient, and so that is what we are trying to be careful about, opening that door to over-utilization or misapplication of medicine. It is important to coordinate care, goodness, yes, but how about making that part of pay-for-performance or finding other ways to coordinate the care.

MR. GREEN. One of the suggestions I know--in fact, we are having enough trouble dealing with our lobbying reform, much less looking too much at the physicians situation, but on the electronic records technology that is something that has obviously a greater good. Not that a doctor having immediate access to the test, but if we are looking at the good as a whole, is there a way that we can draft something if we are trying to actually have that that maybe we would not run afoul of those whether it is IBM or whoever is selling this equipment that they do not all decide that is the one.

I know one of the suggestions I heard is that, for example, for the greater good we might want to have some non-profit or maybe the medical society in a given community or a State saying this is the

depository, this is the information, and anyone who is a member, for example, could then access that without someone feeling like maybe they are utilizing that.

MR. VAUGHAN. I mean a way to deal that you would not have to change any laws or get any IG opinions is if people have some money and they want to encourage the spread of this technology to doctors in a State who maybe do not have the resources or behind the eight ball on it, give it to a foundation, Robert Wood Johnson or some State foundation and they would give out the money. I think you will find a lot of opposition or objections to that idea, and that should tell you something. The people who want to give this hardware and software, they want a tie with that doctor. They want a tie that binds so that that doctor will send patients to that hospital. Coordinating care with the patients is great, but if that hospital that gives the data or the software, is it the best place for that patient.

MR. GREEN. I see I am out of time. Mr. Chairman, if you would allow me just to ask if anyone else on the panel would like to respond.

MR. DETMER. Yes. I just wanted to weigh in on this. Right now our biggest challenge in the U.S. is particularly the small provider office. That is really our biggest challenge. The hospitals, frankly, are getting there and they are building their systems. The thing is our country is a very complex, large place, and I think some of these issues are working, do work, can work, and will work in some settings, but in other settings that opportunity and that kind of option is just maybe going to be very hard to put in play. I think what we are really advocating for, if we can get the regulations right, security and those kinds of design features. Then our feeling is to have this connectivity means that actually a doctor in West Bicycle, Texas can easily get a consultation with the Mayo Clinic electronically, as easy as they can actually with the provider that maybe gave them that connection.

In actual fact I think it is that kind of connectivity that really has significant offsets in terms of these arrangements. So I would like to think you could craft it. I certainly hope you could craft it because I think we need it.

MR. GREEN. Thank you, Mr. Chairman.

MR. DEAL. Thank you. I believe we will start a second round. Is that okay with you all? Okay. Let me start it off. I am going to try to simplify because I think of it in rather simplistic terms, in terms of the problems that I see are encountered. First of all, with regard to a hospital sharing its software with physicians, virtually all of my physicians practice in only one hospital. It does not make a whole lot of sense to me that they should not have some way when the patient goes to the hospital instead of asking the patient when he comes back to the doctor's office,

well, what did they tell you. It sort of reminds me of a story of one of my clients. I asked him one time, I said, well, what did the doctor tell you? He said I have no idea. I do not even think he spoke English.

We have got to have a better way of transmitting information that helps the patient. The one situation, the hospital sharing what their tests were, what their findings were back with the treating physician, he needs to know that. Also, let us suppose there is a consult with a specialist in the same community who does something. He prescribes some medication. Instead of the patient then going back to his primary doctor and being asked, well, what did he give you? Well, I do not really know. What did he tell you? I am not really sure. I did not understand all that. There has to be a better way of doing this. Now there are several things that pop out to me as major problems of what I am talking about. We have alluded to them in some of your testimony.

One is the coding and whether we are talking about the ICD-9 versus the ICD-10. Mr. Mertz alluded to some of the potential problems with the additional codings that are there. Let us talk about that for just a minute. How many of you believe we should go to a broader coding such as the ICD-10? Would anybody care to comment? Dr. Detmer.

MR. DETMER. Yes. Actually I am actually a fellow of the American College of Sports Medicine, and you held up your sheet talking about some of these sports issues. I practiced surgery, vascular surgery, as well as sports medicine for about 25 years, and for 15 years I published a fair amount of work that was internationally verified as being valid. To this day, the coding words or the diagnosis I made in athletes, sometimes Olympic athletes, still does not exist in ICD-9, as well as being able to for payment purposes, I would have to find a code that is sort of related to the leg. In actual fact, what works for billing does not capture what you really need to really try to do research as well as even just talk about. For example, asthma today does not have a lot of the codes in 9 that really are in 10. So there is a set of these.

We do not know how slippery this all is because it is very hard to track down. But suffice it to say there has been a lot of progress in medicine in 23 years, and that is how old that coding system is. So, yes, it does create problems. We not only need to worry about 10, but that is why I talked about the National Library of Medicine. We need to put in this process that can keep that going over time so that we do not have these very tough dislocations every ten or so years. We really need to put in process something that will catch us up but then hopefully keep us up.

MR. DEAL. Mr. Mertz.

MR. MERTZ. Yes. Just briefly on that. ACLA labs, we support moving to the ICD-10, but I would just remind you, first of all, you are

going from 12,000 or 13,000 codes to 120,000 codes, so it is ten times as complex. You may recall that we are just now after four or five years finally adjusting to the HIPAA transaction codes, the new claim standards that took us years to get that. That was much less complicated than moving to this. We almost had a train wreck where providers were not going to get paid by payers because of the complexity of it. So we just want to make sure as we move to this, two years is not enough. We need at least five years to train the people on new systems.

We have to train all of the doctors who submit the diagnosis to us. They are going to have to put eight or ten times as much information on the form that the doctor sends to the lab. If every T is not crossed and every I is not dotted, we do not get paid. We perform the test. We do no get paid, and the system will really shut down. So I would just urge some caution in having a long enough transition period so that we can go there.

MR. DEAL. Yes, Dr. Braithwaite.

MR. BRAITHWAITE. Mr. Chairman, I think that many of the systems that are in electronic health record systems today are based on these coding systems. We get paid for practicing medicine when we submit a certain code. The problem is that those codes are very broad, they are very general, and they do not really reflect, this is what Dr. Detmer said, what is actually done to the patient. If we cannot come up with a coding system that is detailed enough so that what we record in our electronic health systems actually represents what is done to the patient, then we cannot even look forward to that vision I put forward about how we can practice medicine better in the future by actually having computers help us to interpret what those codes mean with respect to the rest of the data about that patient, not necessarily ICD-10, SNOMED CT is a national coding system for example that has that level of clinical information.

As we implement electronic health record systems we now have computers to help us to come up with the right code. It does not have to be done manually out of a book with pen and paper as it is done now in most places for ICD. So I think there is a good balance.

MR. DETMER. You also mentioned the importance of the patient being in play here, and if you have terminology where the patient can see some of these codes that do not really reflect particularly what happened you really help bring that patient into that care environment.

MR. DEAL. Very good points. Ms. Capps.

MS. CAPPS. Thank you again, and you are talking about barriers of some kind and maybe we need to pursue that line of questioning that you started, Mr. Chairman, but I want to see about HIT implementation, what barriers there might be there. And I will continue with you, Dr. Braithwaite. Everyone seems to agree that adoption of electronic health

records and a move toward interoperability would allow different providers, health plans, labs, and others to talk to each other, and that that is a good thing. It would improve quality, save resources, eliminate harmful errors.

Yet, a recent Rand study found only about 20 to 25 percent of hospitals and 15 to 20 percent of physicians offices have an HIT system. Talk a little bit more, I know we brought this up, but focus in on barriers to implementation. And if we design some legislation, we are going to hopefully have a study, but what should we do or could we do that might help get past some of those barriers? And anyone else can jump in as well.

MR. BRAITHWAITE. Well, as I mentioned, one of the major barriers is the incentive system. We are reimbursed in the system for piece work. We are not reimbursed for the health of the patient. And so coming up with several different mechanisms to incent the appropriate implementation of health information technology in the clinical practice would be appropriate. I think in surveys that we have done, people have problems with up front funding as has been discussed. The capitalization of this in practices that do not really have that much capital is difficult. Coming up with the changes in the reimbursement policies so that, for example, a pay-for-performance program under Medicare that actually paid for improved outcomes of the patient based on the data that is produced from an electronic health system would in fact encourage the physicians to get information technology in their clinics and provide higher quality care, as long as the result was not that their incomes actually went down because of these strange reimbursement policies that come out sometimes.

I think in aligning incentives so that the people who purchase the systems and the people who benefit from them are appropriately aligned with the implementation of health information technology.

MR. MERTZ. May I address that? As I mentioned in my statement, some of our national labs, they are connected with about 50 percent of the physician offices, and the figure that was given is right. It costs $30,000 to $50,000 to create this conductivity with the physician office. It is not just the hardware and the software but the training, marrying all the different systems. It is extremely complicated. Half of the offices that we do not have relationships with tend to be the smaller practices where they do not have the resources to do it.

The labs, we have been the ones who invested millions and millions of dollars. We pay for this conductivity. But you get to a small physician office, and they do not have the volume of lab tests to make it economical for the labs to make a $50,000 investment so that they can order the results of their tests and get the results electronically. So that

is, I think, one of the key areas where help is needed to provide incentives and resources. We get paid for doing the test. We do not get paid for spending $50,000 to hook them up electronically. So that is where we need some help.

MR. NEAMAN. If I could just comment from the perspective of somebody that has done it and been there, I think half of the issues relate to financing, where are you going to find the money to do it.

MS. CAPPS. Right.

MR. NEAMAN. The other half relates to the huge behavioral changes for electronic medical records, and the hospitals and the doctor's offices--

MS. CAPPS. Behavior changes by whom, everybody?

MR. NEAMAN. Every clinician, every nurse, every physician, every technologist under an electronic medical records system must change the way they practice. It is no longer writing things out by hand or trying to decipher the physician's handwriting. Everything changes, and for the most part it changes for the better.

MS. CAPPS. Several of you have mentioned incentives. Voluntary, is that sufficient? If we are the ones who would design legislation, is it significant enough for our national interest to mandate some things, or are we even to the point of talking about that?

MR. NEAMAN. I think, from the providers' side, the hospitals and the physicians lack trust. If there is going to be anywhere near the sufficient level of funding to bring doctor offices or hospitals up when we are facing another $36 billion of Medicare cuts.

MS. CAPPS. I hear you on that one.

MR. NEAMAN. I think it is going to have to be again some kind of opportunity included in the private sector to invest monies to make this a real reality, unless the Congress wants to take on a project like rebuilding the Federal highway system of hundreds of billions of dollars to really make this a reality in the near future.

MR. DETMER. I think I would like to comment on that, I think that puts tension in this, as it is not like there is an EHR system.

MS. CAPPS. Right.

MR. DETMER. In fact, there have been some very good studies done that show that if you go for EHR light, in other words, the cheapest kind of way to just get something in, you do not have the decision support infrastructure where you really get your quality, safety, and your ROI pay back. By one calculus of that, if you are willing and can find the scratch to pay four times more you will get 12 times back. So it is not like it is just sort of the thing to do. And so education and change management is a major piece of this. The other thing that I want to echo,

again, that I mentioned earlier in my testimony has to do with authentication.

It was interesting, the day that the commission report on systemic interoperability was put out, and I was on that commission, we happened to have our annual meeting. The same afternoon we had a presentation of some of the folks that were on the commission and talking about it. A woman in the audience said I have a problem for you. She says I am Mary Smith. I have a problem with authentication.

MS. CAPPS. Great.

MR. DETMER. She says I get other people's bank statements when I do on line banking. I need some unique way both for my protection as well as for everybody else's to identify who that is. This issue of being able to have at least a national way of uniquely identifying folks is really something that is a barrier that, again I think is a Federal issue if we are going to address it. Thank you.

MS. CAPPS. And I know I have overstayed my time but this is our last round. I started out by talking as a nurse about patient safety and the benefits of IT. Somewhere in our study, I would hope we could find some way of demonstrating that in the long run the initial outlays will be significant of resources. There ought to be a pay back to society at least for mortality rates dropping, and I would--we get to that as IT--can the study even demonstrate some things?

MR. NEAMAN. In our studies, we can tell you that right now. It does not take a long term. We have shown in our studies in our hospitals, our doctor offices, there is a payback, economic, clinical, saving lives. It works. It absolutely works.

MS. CAPPS. And is there demonstration of that already?

MR. NEAMAN. In our system, yes.

MR. DETMER. Speaking of the nurse and the education challenge, the strategy we really need is educating nurses in particular.

MS. CAPPS. I do not believe we will end up doing all of this, not all of it, but a fair amount of it at least in the--

MR. NEAMAN. If I might, just get a lot of great benefit out of it too.

MS. CAPPS. I should say.

MR. NEAMAN. Better care. In our studies we saved 20 percent of the nurse's time instead of babysitting the chart and trying to decipher the doctor's handwriting.

MS. CAPPS. And you are all talking about it in acute care probably, but look at long-term care and who delivers that care and who has to take a huge chunk out of every hour of patient care to documenting.

MR. NEAMAN. Absolutely.

MR. DEAL. Let me go to Dr. Burgess next.

MS. CAPPS. It is tough for the doctors, isn't it? Thank you.

MR. DEAL. Dr. Burgess.

MR. BURGESS. You know, I think back over 25 years of medical practice, the two things that came out of Washington that destroyed a better part of the joy of life were the Stark laws and HIPAA, and I cannot help but feel we are today with the grand daddy of them all, and I do worry about what the world will look like so it is terribly important for us to get that right. So with that sort of onus, Mr. Mertz, I interrupted you before. Let me let you finish what you were trying to tell me about the Stark laws.

MR. MERTZ. Well, actually the point I was trying to make, I eventually made which was that it is a sizable investment, $50,000 or so, to set up that conductivity between the labs and the physician offices. So it is going to take a lot of money and the labs have made that investment. I just want to reiterate, we very much support the Stark law in many ways because it does not allow the abuses that happened many, many years ago. We are able to only provide the equipment that is needed just very narrowly to ordering tests and reporting results.

But we see the need to expand it a little bit to allow more investment and IT. We just want to make sure that we are still included in an exemption, but that it is done carefully. So I appreciate the opportunity to finish up. Thank you.

MR. BURGESS. And, Mr. Vaughan, on that, does it ever increase the cost of care to not share information?

MR. VAUGHAN. Sure.

MR. BURGESS. I can tell you in my hometown of Denton, Texas that I encounter that situation every day where they've got two hospitals that are competing, and not only do they not communicate with each other, they are forbidden from communicating with each other. So a CAT scan in one hospital on a Friday night means you get a CAT scan in the next hospital if you go into the other emergency room on the next Friday night because you did not like the care you got across town. It is a system that creates more expenditure, I believe, by not communicating.

MR. VAUGHAN. Absolutely. This is where so much of the savings will be, but how you can get this information, the software, the hardware, into doctors offices, how can we do it where it does not lead to some distortions that we might not even see for a while where one hospital that has got good cash flow in a year, the other one has been doing charity care, might be a little starved. This one donates some stuff. Just consciously or unconsciously doctors will say I like those guys. They have been helping me. They have been helping my office. I move my patients there and they may not have the best department and everything.

So you get those goofy, almost unconscious distortions, can't we pay for this up front? I know with the Federal budget situation, you know, get a life. There is no cash lying around.

MR. BURGESS. Mr. Neaman has found the savings for us in the Medicare, is that what you just told us a minute ago?

MR. NEAMAN. In our system, yes.

MR. BURGESS. So how much money are you going to save us? If the Chairman and I are successful in getting this done and your company is the one that gets the contract, are we going to save that $34 billion in Medicare this year that we can then turn back over?

MR. NEAMAN. I can only comment on our system and what we have actually found. The point being is that the systems that we have experienced really do save lives and they do less testing, not more testing, and they protect patients from abuses of testing. We have even shown in our studies that the efficiency improves so much that we were able to save cost-wise $17 million a year in our system by doing things right the first time, not having to do them time and time and time again, so there is a small incremental savings once you get the system up and running.

Again, all the other benefits are tremendous. I think Mr. Vaughan's examples might be a little confused with what the real issues are here. In the examples of over-testing, such as too many lab tests or too many X-rays when a physician owns that equipment, that is not what we are talking about here. If you want to preclude that, then do not let physicians own MRI machines, a whole other issue.

MR. BURGESS. It is not a good idea, by the way, but continue.

MR. NEAMAN. I was not advocating it as a principle, particularly my orthopedic surgeons would let me know about that. But what we are talking about here is the sharing of data, and shouldn't we be focused on the patient here, to share that data between our hospitals and our physicians. Doesn't the American public expect our hospitals and doctors to work together around a central point of data? The answer is quite clear in our experience. Absolutely yes.

MR. BURGESS. Mr. Pyles.

MR. PYLES. I have been wanting to get this in. You asked a question in your last round, and I think it touches on what you are asking now. How much you save I think is going to depend on how much you need. The numbers I have seen on the cost of wiring the country for health IT are $176 billion initially as start up-front costs and $46 billion annually. Now keep in mind you are going to have to replace that information system. They have a life span of about, as I understand it, three to four years, so you are going to be continually replacing them.

It is not to say you should not do it, but when you are talking about a solo practitioner in Shady Side, Maryland where my family physician is, that is a big chunk. His share of that is a big chunk. He was chosen actually as one of 200 physicians in Maryland to use an electronic information system by Blue Cross. He has found that it is out of order. He carried around a little box that he is supposed to input information in. He cannot communicate with the system, at least a minimum of three times a day, and the information he gets back is often times so garbled he cannot understand it. So he is a little frustrated. I have heard healthcare is the last area where we do not have IT. It may not be such a bad thing because we are dealing with people's lives, and we would not impose a drug or a procedure on the public unless it was proven safe and effective for patient use. So I would just urge you to be careful.

As a lawyer, one of the questions I have always had too is what is the standard of care for an electronic health information system? When you go into the hospital and a patient has a seizure you punch the screen to get the patient's current status and what they are on, and it says access denied and you prescribe something and the patient dies. What is the standard of liability there? A judge is going to have to figure that out. Were you negligent? Was the hospital negligent? Was it expected for the system to be down once a week, once a month, once a year? My computer is down a minimum of twice a week. Maybe these systems are more reliable but that is a whole area that is completely unexplored as far as I can tell. I do not see any standard of care like a Xerox standard. Xerox will tell you the copier machine will never be down more than four hours.

MR. BURGESS. Can Dr. Detmer respond, Mr. Chairman?

MR. DEAL. Sure.

MR. DETMER. I agree with him on one point, and I disagree with him on another. I agree with him that IT is not some kind of magic. It has got to be done right for it to work, and we have heard from some places that are doing it right, and, boy, it does work. That is why this education issue is also a huge piece of this, because if you just try to do it, I am not sure in fact you will ever see a ROI.

On the other hand, if you do it right I think we now do have enough body of evidence to be able to speak to safety, efficiency, cost effectiveness, patient centeredness, timeliness. As prices drop, you do start improving equity as well, and that is a U.S. problem.

MR. DEAL. Why don't we let Mr. Nelson defend his industry?

MR. NELSON. I think the comment that I would make is we've got to keep in mind that the bulk of the healthcare dollar really goes to chronic disease, and there are not a lot of them. Interesting, you know, there is various data out there to support this, but the average patient when we

get down to actually looking at it on a by patient basis, they have on average between five and ten physicians if you have a chronic disease. Those doctors do not talk to each other. So it is real obvious that the only way that we are going to actually make that work and reduce the redundant tests and improve the quality of medical errors and all that is if we give smart people information so that they can make smart decisions, but allow those smart people and physicians, I think as Dr. Burgess mentioned earlier, it has got to be in a way so that the physician is not penalized in the process.

We got 16 percent of the gross national product right now going to healthcare which is far over any other country in the world. Any other outcomes are not even in the top ten right now, you know. I think it is a shifting of the dollar that we are talking about. Medicare and Medicaid employers and payers are the ones that are the biggest beneficiaries of these systems, and we shift the dollars to some extent from there to the primary care physician, which are the guys who really I think are in control of the healthcare system today.

MR. DEAL. Well, thank you.

MR. BURGESS. Mr. Chairman, could I ask a question?

MR. DEAL. Sure.

MR. BURGESS. We are going to have a bill before us either in this subcommittee or the full committee about this, and if it would not be out of order to ask each of our respondents to give us their impressions about what they like, what they dislike about the bill. This is important that we get it right because this could be the headache for the next two or three generations of physicians or the benefit for the next two or three generations of physicians.

MR. DEAL. Certainly. That would be appropriate, and there may be other questions from other members of our committee that were not here that may be submitted to you in writing. We would appreciate your response on that. I commend all of you. Somewhat different points of view on some issues, but generally I think there is a consensus that this is an area that is worth exploring. It is worth us trying to move forward on the issue. We appreciate your various points of view. As Dr. Burgess indicated, if we can move a legislative agenda, we would appreciate your further comments with regard to that as we attempt to refine those. We do appreciate your time, and thank you for your attention and your being with us on this occasion. I am not going to adjourn the hearing because we expect to have in the next few weeks a follow-up panel that will be from a Federal point of view and so therefore in light of the fact that that further panel will elaborate on the same general issue, we will simply just suspend this session of the hearing on IT. Thank you all for being here.

[Whereupon, at 1:56 p.m., the Subcommittee adjourned.]

RESPONSE FOR THE RECORD BY WILLIAM BRAITHWAITE, MD, PHD, CHIEF CLINICAL OFFICER, EHEALTH INITIATIVE AND FOUNDATION FOR EHEALTH INITATIVE

Responses to Questions following March 16, 2006 Subcommittee on Health Hearing entitled: "Legislative Proposals to Promote Electronic Health Records and a Smarter Information System"

1. How important is it to think realistically and not try to do everything at once in terms of a complete electronic medical record, but instead focus on things like e-prescribing, lab results, and patient information?

Through eHI's Working Group for Value Creation, Working Group for Practice Transformation and other organizational efforts, eHI is exploring important issues in this topic area. To the question specifically, trying to do everything at once in terms of a complete electronic medical record, to me, is like trying to boil the ocean. Although an electronic health record system for every clinician, including functional clinical decision support systems, is a necessary vision and goal to work toward, this development and implementation process will take decades to complete. It is much better to implement some "low hanging fruit" for which a return on the investment can be demonstrated as a way to support the longer term effort.

To the functions you mentioned, e-prescribing, lab results, and patient information, I would add medication history (including allergies) and clinical reports to complete the set of commonly mentioned electronic health information exchange functions that clinicians agree would help provide higher quality healthcare in the short term.

2. Can you give an example of some of the decision support systems that are possible by moving towards smarter information systems?

Some examples of decision support functions include:

- Advising a clinician that a drug he/she is trying to prescribe has contraindications that must be considered (and possibly explained or justified) such as allergies, potential drug-drug interactions, instance of another prescription or OTC drug the patient is taking with similar physiological activity and existence of a less expensive alternative with similar activity.
- Advising a clinician that a lab test that he/she is trying to order was done recently on the same patient and present the results of that test for consideration to avoid redundant procedures.
- Advising a clinician that a result of a test (laboratory, radiology, pathology, or other) indicates an abnormality that has not been documented and/or acted upon.
- Advising a clinician that a screening or follow-up test judged to be appropriate for the particular patient (age, weight, sex, diagnoses, health status, etc.) has not yet been ordered or has been ordered but not produced a result in the expected timeframe (e.g., results of ordered Hgb A1c test have not been received within 2 weeks of follow-up patient visit for diabetes control).
- Advising a patient that a refill of a prescription for a drug that should be taken daily to treat a chronic disease is overdue.

RESPONSE FOR THE RECORD BY ALAN MERTZ, PRESIDENT, AMERICAN CLINICAL LABORATORY ASSOCIATION

April 18, 2006

The Honorable Nathan Deal
Chairman, Subcommittee on Health
House Energy & Commerce Committee
2125 Rayburn House Office Building
Washington, D.C. 20515-6115

Dear Chairman Deal:

Thank you for the opportunity to testify before the Subcommittee on Health at the March 16, 2006 hearing entitled, "Legislative Proposals to Promote Electronic Health Records and a Smarter Information System." Per your request, attached are answers to the questions posed in the April 11th letter to the American Clinical Laboratory Association (ACLA).

The Honorable Nathan Deal

1. **What particular function of healthcare do labs provide that makes them a good starting ground for smarter health information systems?** Laboratory data are the heart of the medical record. Laboratory data represent 60-70% of the medical record while comprising only 5% of total hospital costs and only 1.6% of Medicare costs. The vital information provided by laboratory data directs the diagnosis and treatment of disease, improves the efficiency of the clinical care provided, and most importantly, improves clinical outcomes for patients. The long-term benefit of these effects is reduced health care costs. For instance, 62% of the Health Plan Employer Data and Information Set (HEDIS) effectiveness of care measures are informed by diagnostic tests. Diagnostic tests are specified as important to measure in 80% of the clinical evidence based guidelines for the most costly disease conditions in the U.S. It is for these reasons that virtually every health care community trying to develop an electronic health information infrastructure is looking to laboratories first. In a survey of hospitals, the number one health care information technology (IT) function in use by the majority of hospitals today is the electronic order entry and review of results for diagnostic services. For example, ACLA member Quest Diagnostics, a commercial laboratory with business relationships with over half of the nation's physicians and hospitals, currently sends 60% of its results and gets 40% of orders via the Internet. The investment that laboratories have made in health IT also includes public health – ACLA member companies report to over 3,000 public health agencies at the local, regional, and national level – much of which is done via electronic means.
2. **I understand that labs have a limited exception under the Stark law. Can you explain how this exception works and whether there are any examples of abuse in this area with respect to labs?** The terms of the Stark law are defined to exclude from the law's scope the provision of hardware or software by a clinical laboratory to an ordering clinician provided such items are "used solely to order or communicate the results of tests or procedures for such

entity." This provision was added to the Stark law when it was amended by Congress in 1993. Under the terms of this provision, laboratories are not permitted to include other types of functionality in the hardware or software they are providing to the ordering physician without charging fair market value for this added functionality. For example, one of ACLA's members currently offers a product which, in addition to being able to order tests and transmit results, also enables the physician the means to electronically order prescription drugs. Due to the limited nature of the Stark law provision discussed above, this laboratory must charge fair market value to the participating physician for this additional e-prescribing functionality. The laboratory provision has helped shepherd health information technology into numerous physician offices and hospitals throughout the country today. The ability to provide clinicians with this limited hardware and software is fundamental to rendering efficient, comprehensive laboratory services to patients - a critically important function that must be maintained. Clinicians place a high value on being able to order laboratory services and receive laboratory results electronically because it improves legibility, decreases error rates, produces more timely results, and allows the monitoring of redundant or duplicative testing. ACLA member laboratories strive to fully comply with the parameters of the Stark law and we are not aware of any examples of abuse in this area.

3. **With respect to ICD-9/ICD-10 issues, would it be safe to say that we would get more detailed and accurate information by switching to ICD-10? If yes, why have we been so slow to move toward this code change?** Transition from ICD-9 to ICD-10 does hold great promise – provided clinicians accurately use the more detailed diagnosis and procedure codes offered by the ICD-10 Clinical Modification (CM) and Procedural Coding System (or PCS). More detailed procedure codes could allow for enhanced tracking and analysis of clinical and economic benefits and better outcomes research. However, the transition to ICD-10 has justifiably been slow due to the massive overhaul to providers and payers' computer systems, and the time and expense needed to provide appropriate client education, training and testing of the new systems. This transition would be particularly difficult for laboratories since they bill Medicare directly, yet depend on the ordering physician for the diagnosis codes to include on the claim they submit to Medicare. While the current iteration of ICD-9 consists of roughly 13,000 diagnosis codes, problems persist today with physicians not providing the appropriate ICD-9 codes in order for laboratories to get paid. ICD-10's 120,000 codes have the potential for delays in reimbursement if providers are not well educated on how to use the new system. Finally, other regulatory changes (including the replacement of Version 5010 of the 837 claim standard) must occur before ICD-10-CM can be implemented

4. **Having uniform standards for the transmission of laboratory results is an essential part of promoting electronic health records and a smarter health IT system. Can you share with the Subcommittee what progress has been made in establishing such uniform standards?** Much work has already been accomplished in developing uniform standards for laboratory result reporting. Currently, most laboratories and other diagnostic services use HL7 to send their results electronically from their reporting systems to their care systems. In that transmission most laboratories utilize Logical Observation Identifiers Names and Codes (LOINC) to facilitate the exchange and pooling of results, such as blood hemoglobin or serum potassium for clinical care, outcomes management, and research. The laboratory portion of the LOINC database contains the categories of chemistry, hematology, serology, microbiology (including

parasitology and virology), and toxicology. The Consolidated Health Informatics (CHI) initiative, one of the Office of Management and Budget's eGov initiatives adopted LOINC as one of its core uniform standards on March 21, 2003. However, what is also needed is an implementation guide for this system, given the variability among laboratories in reporting different LOINC codes for the same test (there are over 25,000 LOINC codes for laboratory tests). The EHR-Lab Interoperability and Connectivity Standards (ELINCS) project, a non-proprietary effort involving various players within the health care delivery system (including those focused on the transmission of lab results), has been doing just that. In March of 2005, ELINCS, through the leadership of the California Healthcare Foundation, began developing an implementation guide to 'map' the top 80% of performed laboratory tests. This 'mapping' essentially creates uniformity among laboratories, providers and vendors alike in terms of which LOINC codes refer to which laboratory results. The initial effort was completed in late 2005 (v1.0) and additional work on v2.0 is nearing completion, which expands the project to cover the top 95% of all performed tests (around 170 tests). In September of 2005 the Certification Commission for Health Information Technology (CCHIT), which was awarded an HHS contract for health IT product certification, included ELINCS v1.0 among the handful of interoperability specifications it has proposed for its first round of certification criteria for electronic health record systems.

5. **Establishing an electronic connection between labs and physicians or hospitals for ordering tests and receiving results can be very costly. This cost is a significant barrier for many physician offices, particularly smaller practices. How costly is it to establish such interfaces, why is it so costly, and what is the impact on health care practices?** The eHealth Initiative, in a recent report entitled, "Practice and Laboratory Connectivity," estimated that establishing custom interfaces between physicians, hospitals and laboratories can cost anywhere between $30,000 to $50,000. This high cost is due to two factors: (1) the cost of the actual hardware/software, installation and training of staff; and (2) the cost to "marry' the existing data streams of the participating provider and the laboratory. This cost burden, most often paid to a vendor, is the direct result of the lack of uniform electronic test requisition and result reporting standards. Due to the significant cost involved with establishing this connectivity, the provision of this technology is a business decision – one which often times prevents this technology from reaching both rural and small physician/hospital locations. However, with the ongoing work of the ELINCS project in creating an implementation guide for electronic results reporting (and plans to tackle the test requisition in the near future), it is our hope that in the next few years the cost prohibitive nature of custom interfaces will abate, thereby leading to greater access to this technology for physicians/hospitals both in rural areas and in smaller practices.

Thank you once again for the opportunity to testify before the Subcommittee. If you have questions or need any additional information, please do not hesitate to contact me.

Sincerely,

Alan Mertz
President

RESPONSE FOR THE RECORD BY MARK NEAMAN, PRESIDENT AND CEO, EVANSTON NORTHWESTERN HEALTHCARE, ON BEHALF OF HEALTHCARE LEADERSHIP COUNCIL

EVANSTON NORTHWESTERN HEALTHCARE

Mark R. Neaman, FACHE
President and Chief Executive Officer

1301 Central Street, Evanston, Illinois 60201
(847) 570-5005 (847) 570-5179 fax
mneaman@enh.org

May 5, 2006

The Honorable Nathan Deal
Chairman, Subcommittee on Health
House Energy and Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Deal:

Thank you for the opportunity to testify before the Subcommittee on Health at the recent hearing, "Legislative Proposals to Promote Electronic Health Records and a Smarter Information System." It is my pleasure to respond to your follow up questions. As directed, both the questions and answers are below.

1. Can you give any real-life examples of how inconsistent state privacy laws could affect the vision of having a nationwide interoperable electronic medical record system?

As outlined in my testimony, health care providers and plans must comply with the HIPAA Privacy and Security Regulations as well as state laws that are contrary to and more stringent than the federal standard. However, in addition to complying with the state laws in the state where a provider is located, providers must also comply with the laws of other states that contain additional variances.

For example: Though laws requiring patient consent for disclosure of information regarding one particular condition are similar, providers in Pennsylvania and New York could not simply substitute a similar consent for the other state's and thus must track and utilize different consent forms for practitioners, specialists, hospitals, plans, PBMs and others who may be located in either state.

Below are a few examples of actual variances in the requirements for each consent form:

New York	Pennsylvania
Consent form must be established and approved by the New York Department of Health.	Consent form must include statement that information has been disclosed from records protected by Pennsylvania law.
Must include the name of the person to whom the information is being disclosed.	Allows the title or organization to substitute for the name of the individual to whom the information is being disclosed.
	Must also include the name of the person authorized to make the disclosure.
Must include time of expiration of the consent.	Allows a listed event or condition to cause the consent to expire, rather than requiring a specific date.
	Must include information about how much and what kind of information will be disclosed.

These are just a few of the variances between consent forms in neighboring states. As you can see from the above requirements, such a consent form would be necessary for almost any use of information regarding this particular condition. Multiplying these variances by the number of times a consent would be required for additional uses of the same patient's information, state laws on other conditions, the number of patients, and the number of providers and plans who must comply with these state laws, and the substantial amount of time necessary to track and comply with the constantly changing state laws and regulations becomes a huge disincentive to participation in a national or regional health network.

2. Can you explain how an exception to the Stark and Anti-Kickback laws would help hospitals and providers coordinate health care for patients?

Here is a simple example of how an exception to the Stark and Anti-Kickback laws would help Evanston Northwestern Healthcare (ENH) coordinate care. Currently ENH can provide "employed" physicians with the software and computer hardware necessary for our Electronic Health Records system because of the "employee" exception to the Stark & Anti-Kickback statutes. However, ENH cannot provide this to independent physicians who admit patients to our hospitals. Allowing us an exception to assist physicians with IT needs would spur broader adoption of the EHR along the continuum of care between hospitals, physicians, etc. In this way, patients – either pre-admission or post-admission – would benefit from the open communication of all treating providers.

3. I applaud you for implementing an electronic medical record at your hospital. We in Congress do not want to hinder activities that are already being done in the private market. In your opinion, what kinds of things could Congress do to be helpful and not hinder the further advancement of your system?

Evanston Northwestern Healthcare and Healthcare Leadership Council (HLC) believe that the Federal government should continue to oversee a comprehensive program of health data and information standards development that will facilitate exchanges and sharing of data and information. Such standards will foster smooth and efficient communications and cooperation, regardless of individual system structure or architecture.

However, we would be concerned about legislation that was too prescriptive in overseeing the standards development process. Requirements that do not allow for the public/private partnership and multi-stakeholder participation currently exhibited in efforts such as the National Quality Forum would be too inflexible.

A benefit of the public/private process and absence of prescriptive legislation is that efforts to craft standards are timely and responsive to future technological development. By contrast, the timeliness achieved by unilateral action of the federal government sacrifices process for the achievement of a deadline.

It is important to note that the development of some standards will necessitate action by the federal government. As you know, HLC and Evanston Northwestern Healthcare support a federally uniform standard for privacy and security laws and regulations. In

order to provide for such a standard, the federal government must act to preempt conflicting state regulations and laws.

Another area, which requires federal action, is the need for the Federal government to implement financing mechanisms to spur private sector HIT investment. This financing will accelerate the widespread adoption of HIT.

Such financing would ease the financing crisis facing those attempting to adopt and implement often high-cost, highly complex HIT. Financing mechanisms could include: payment "rewards" or "add-ons;" creation of an HIT revolving loan fund to invest public dollars in HIT projects and programs (e.g., modeled after the "Hill Burton" program); a revolving loan fund with debt forgiveness in accordance with specified criteria such as savings to the Medicare trust fund; tax incentives; reimbursement incentives based on improved patient outcomes; and matching private funds with public funds through grants from the Department of Health and Human Services and the Department of Homeland Security.

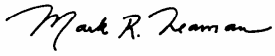
Another important aspect of federal financing is the above-mentioned relief from federal Stark and Anti-Kickback laws. Modifications to these laws are an essential component of a federal financing effort, providing a way that hospitals and providers can collaborate in developing interoperable health information technology systems.

As a caution, federal grants and loans must not be fraught with onerous requirements that will make their acceptance impossible by smaller health providers with scarce resources.

These are just a few examples of areas in which action by the federal government will be a help or "hindrance."

I hope this additional information is helpful to you as you and your Subcommittee deliberate on HIT legislation. Please feel free to call on HLC or me if we may be of further assistance.

Sincerely,



Mark R. Neaman
President and Chief Executive Officer
Evanston Northwestern Healthcare
Chairman
Healthcare Leadership Council

RESPONSE FOR THE RECORD BY JAMES C. PYLES, ATTORNEY MEMBER, POWERS, PYLES, SUTTER AND VERVILLE, P.C.

April 25, 2006

Dear Mr. Grant,

Please accept my response to the letter from Chairman Deal of April 11. I was unable to respond to the letter when it arrived because I was completing the petition for certiorari to the Supreme Court in Citizens for Health v. Leavitt which challenges the constitutionality of the HIPAA Amended Privacy Rule. That petition had to be filed on April 13, and I had to be out of the office until this week. My secretary reminded me that this was due today. I think you will find the answers helpful.

Question 1:

The question does not accurately state the question I raised. My question was, " Will Congress **compel Americans** to disclose all of their most sensitive health information about themselves and their families to and from a national "interoperable" health information system **without meaningful, informed patient consent, against their will and without adequate enforcement against unauthorized uses and disclosures?**"

The question to me also incorrectly states that "under current health care operations providers may exchange identifiable health information for the purpose of treatment and billing." In fact, the Amended Health Information Privacy Rule that is currently in effect, authorizes covered entities (including doctors, other providers, health plans and health care clearing houses as well as their business associates) to use and disclose virtually any of an individual's identifiable health information for the purposes of treatment, payment and health care operations. These are separate terms and purposes. Treatment and payment are generally defined as uses for the patient's treatment where the patient has requested that treatment and payment where the patient has requested that an insurance claim be filed. So these uses and disclosures are somewhat within the patient's control. Health care operations, by contrast, are a broad list of uses generally for the benefit of the covered entity that are completely outside of the patient's control that include underwriting and premium rating, business planning and development, management activities, and due diligence in connection with the sale of a business. 45 CFR 164. 501, 65 Fed. Reg. at 82,803-04. As the American Medical Association said in its comments on the Amended Rule, "As currently defined, "health care operations" includes a broad array of activities unrelated to a patient's individual treatment or payment and extending far beyond the necessary disclosures and uses patients would expect when they seek health care...**An optional consent provision combined with a broad definition of health care operations would effectively compel patients, as a condition of obtaining health care services, to allow uses and disclosures of their protected health information that are not routine or necessary for a covered entity to run its business."** AMA letter to HHS, p. 7 (April 26, 2002).

The question also states, "Of course, doctors may also not disclose information if they choose or other rules do not constrain it." That choice is not as available as the statement implies. Covered entities may provide a consent process for disclosures for treatment, payment and health care operations, but only by entering into an agreement with the patient to restrict uses and disclosures. 45 CFR 164.522; 67 Fed. Reg. at 53,213. Covered entities are further discouraged from entering into such arrangements because failure to act in accordance with such agreements can result in a violation of the Rule and civil penalties. 67 Fed. Reg. at 53,213.

The statement, however, reveals the real change that the Amended Rule made in the practice of medicine and the right to medical privacy. It is correct that under the Amended Rule, for the first time in the nation's history, covered entities have been given the federal authority to decide whether a patient's health information will be disclosed without the patient's consent and even over the patient's objection. The practice under constitutional law, medical ethics and the laws of most states, prior to the Amended Rule, was for THE PATIENT to be able to decide whether his or her identifiable health information would be disclosed. In other words, a patient's identifiable health information could not be disclosed without the patient's consent. This long established principle was recognized in the Original Health Information Privacy Rule. 65 Fed. Reg. at 82,474.

When many consumers and practitioners raised the concern that the proposed Amended Rule would violate medical ethics and state laws, HHS responded that The Amended Rule was only intended as a "floor" of protections and that more stringent state privacy laws and standards of medical ethics would remain in effect. 67 Fed. Reg. at 53,212. However, the decision making power was taken from the patients and vested solely in the hands of covered entities.

So in answer to the specific question whether current law fails the test, the answer is that the Amended Rule does fail that test to the extent that it authorizes covered entities to disclose Americans' identifiable health information without their consent and against their will. But HHS contends that current law is only a "floor" of privacy protections and was not even intended to be a "best practices" standard. 67 Fed. Reg. at 53,212. Some who testified at the hearing desire for the Amended Rule to become the national privacy standard. The effect would be for the "floor" to also become the "ceiling" which would leave little room for consumers' ethical and constitutional rights to health information privacy. The HIPAA Amended Rule cannot be made the national privacy standard because it essentially eliminates the individual's right to health information privacy rather than protecting it.

Question 2:

Should a patient be able to "block" a doctor who needs to send certain medical information for the purpose of billing?

Answer—A doctor should always act in accordance with standards of medical ethics. The standards of medical ethics of the American Medical Association, as well as virtually every other medical society, state that, "The physician should not reveal confidential communications of information without the express consent of the patient, unless required to do so by law." See Tab 1 to my testimony, item 16.a. HHS also found that this is has been the established practice throughout the history of the country. 65 Fed. Reg. at 82,474.

So if a patient, a Congressman for example, wishes to file an insurance claim for treatment of the flu, he or she should be able to expect that their psychiatric record or genetic test for a predisposition for cancer will not be disclosed without their consent. If the insurance company insists that they have to have the entire medical record to pay the claim, the Congressman should have the right to pay privately and not have to disclose this information against his or her will. If we do not allow patients to assert their traditional right to privacy, they will avoid seeking needed health care and/or instruct their physicians to falsify their medical records. HHS has found that many Americans already are taking such self protective measures and physicians are withholding information from patient records. 65 Fed. Reg. at 82,468. Thus, protection of the right to privacy is essential for effective, high quality health care. See HHS determination to this effect. 65 Fed. Reg. at 82,467.

So the short answer to your question is that a doctor should only be able to disclose a patient's identifiable health information for billing purposes with the patient's consent. If this means that the claim cannot be paid, the patient will have to pay privately (as has always been the case). The physician can determine this, as they always have, by determining prior to providing the services whether the patient will consent to the disclosure of information necessary for insurance coverage or agree to pay privately.

What a physician cannot do in the ethical practice of medicine, is disclose a patient's identifiable health information for billing or other purposes without the patient's consent, unless required to do so by law.

Question 3:

Should a patient be able to edit or block the sharing of identifiable health information between a physician and a specialist?

Answer—Again, we believe in the ethical practice of medicine under which a patient's identifiable health information cannot be disclosed, even to another physician, without the patient's consent. There is no reason why this consent cannot be obtained at the time the patient is accepted for treatment by the first physician. This is not a novel concept. This has been the established practice, as reflected in standards of medical ethics, throughout the history of the country.

For example, psychoanalysts often seek consultations from other practitioners, but they never do so without obtaining the patient's consent. Certainly, no physician, even a physician to whom a patient was referred, would ever treat a patient without his or her consent.

We do believe, however, that there are situations in which a physician should be able to infer consent where it is necessary to carry out treatment that a patient has requested. This is essentially the approach that was taken in the Original Privacy Rule which allowed health care providers in an "indirect treatment relationship" (such as a consult) to review an individual's identifiable health information without express consent. 45 CFR 164.506(a)(2)(i) (65 Fed. Reg. at 82,810).

The point that must be appreciated is that if the individual's right to privacy for identifiable health information is not protected, the information will simply not exist, because the patient will refuse to disclose it. This was expressly recognized by the Supreme Court in Jaffee v. Redmond, 116 S. Ct. 1923, 1929 (1996). That decision has now been followed in over 150 other cases.

The right of consent is not new or novel. It is the core concept of medical ethics and the right of all law abiding citizens "to be let alone" as protected by the First, Fourth, Fifth, Ninth, and Fourteenth Amendments to the Constitution. As HHS has found, the right to privacy is a "fundamental right" of all Americans. 65 Fed. Reg. at 82,464.

Do not hesitate to contact me if you have further questions.

Jim Pyles
On behalf of the American
Psychoanalytic Association

RESPONSE FOR THE RECORD BY DON E. DETMER, PRESIDENT AND CHIEF EXECUTIVE OFFICER, AMERICAN MEDICAL INFORMATICS ASSOCIATION

1. It seems important that when we're talking about electronic health records that we would need to come up with a common medical terminology. Is the licensure of SNOMED the final step in coming up with this common terminology or does more need to be done?

Response: The initial comment is accurate; that is, we need to have a common medical terminology. The licensure of SNOMED was not the final step in coming up with a common terminology and more does need to be done. Today, we have three problems. First, we don't have a global system that brings SNOMED and ICD-10 together and, second, we don't have an agreed-upon manner by which the world will maintain the terminology and classification system going forward. Medicine constantly changes due to new discoveries about human biology and diseases, new technologies, and new treatments. The challenge is to find a way to support those groups who can do this kind of work well and also support a method and manner of giving the world timely open access to the terminology and classification into the future. The USA would be very wise to license SNOMED and subsequent terminology and classification for use by the world and not just for USA institutions from the National Library of Medicine as well as support the ongoing maintenance of the standard terminology and classification systems through the NLM; an extra $6-8 million per year would give the NLM the funding it would need to support this but the benefit to the USA itself would more than offset this cost. A joint task force of AMIA and AHIMA experts is currently working on a white paper that discusses this issue in some detail and a copy of that report will be sent to you as soon as it becomes available. Additional funding for informatics research on this and related issues such as that mentioned in the next paragraph is needed.

The third problem relates to the movement within the USA of giving patients electronic health records populated upon information used in paying insurance claims. The current terminology on insurance claims that used ICD-9 is so outdated that it will only serve as an approximate representation of a person's health status, treatment, or disease condition(s). We have very little data to show us just how well or poorly it reflects reality but many experts are concerned about the potential distribution of millions of records of dubious accuracy and the confusion this will cause physicians as well as patients as they seek to sort out reality from 'billing' data. We will have integrated computer-based personal and clinician health records in the future and this makes the challenge of addressing the remaining terminology and classification issues for now and going forward.

2. You mentioned the need for ways to authenticate or identify individual patients – what are the privacy aspects associated with a unique personal identifiers, as was called for in the original HIPAA legislation?

Response: The privacy aspects of authentication or identification of individual patients fall into two categories based upon what one consider 'privacy rights' to entail in a free society. If 'privacy rights' are defined as a 'right to be left alone', they imply something different than if 'privacy rights' are defined as the 'right to remain unknown'. Since I do not believe a modern society can exist by operating with the second definition as the dominant operating policy, I will respond to policy dimensions relating to the first definition. Indeed, the testimony of one witness at the hearing reflected that latter perspective.

The original HIPAA legislation called for unique personal identifiers for health for a number of reasons. First, all developed economies in the world have adopted this

approach as the most reliable and cost-effective manner of personal identification for health purposes. Today, we are seeing rising interest and indeed rapid movement to give citizens their personal health information. It is crucial for both health care safety and personal privacy that both doctors and patients exchange data solely to those to whom it is intended and no one else. In all likelihood we will use an algorithm in addition to a unique identifier. If one does not have access to a person's social security number (SSN) for example, the accuracy of the algorithm drops considerably. To assure the greatest accuracy, a unique personal identifier is the most sensible approach.

At the minimum we need national public policy that will assign a unique health identifier with an opt-out arrangement for those citizens who fall into the latter category mentioned above. Suggestions have included the SSN plus a four digit PIN and a range of other suggestions have been made. There is ample testimony before the NCVHS on this topic. I see some value for using the first five digits of the SSN plus a four digit PIN that the individual selects.

3. We have heard complaints about the negative impact of the HIPAA privacy rule on clinical research – how would legitimate clinical research uses of information be better facilitated?

This question has many potential responses. Unfortunately, the potential for HIPAA to be revised so that it could better support clinical research without legislation being passed or regulations being developed that would in reality make clinical research even more difficult to undertake is a compelling consideration. In light of this, only one recommendation follows. As the nation moves toward an approach to authenticate all individuals in order to improve patient safety and protect the privacy of their data, the citizen at the time of identifier selection could be given the option of 'ticking a box' to allow him or her to be contacted by researcher(s) having clinical research protocols approved by a legitimate institutional review board to see if the individual had any interest in participating in such a study or studies.

Those citizens who chose neither to have a unique identifier nor participate in research would not be able to be notified but certainly millions of citizens both could and would choose to participate. This would be enormously helpful to the clinical research community. Obviously, those who chose not to collaborate would still gain the benefits from any findings coming from those sharing their data. Of course, if sufficient numbers of people opted out in a certain category of age or sex, no valid research would be achievable since sample sizes might be too small. This creates a problem known as 'free riders'. Too many free riders and the train won't leave the station. If there is interest in other ways to improve clinical research, I can respond further.

Don E. Detmer, MD, MA, President and CEO, American Medical Informatics Association

SUBMISSION FOR THE RECORD BY THE BLUE CROSS AND BLUE SHIELD ASSOCIATION

Introduction

The Blue Cross and Blue Shield Association (BCBSA) appreciates the opportunity to provide testimony to the Committee on H.R. 4157, the Health Information Technology Promotion Act of 2005, and applauds the effort to facilitate and encourage the widespread adoption of health information technology (health IT).

BCBSA is made up of 38 independent, locally operated Blue Cross and Blue Shield companies that collectively provide healthcare coverage for more than 93 million people – nearly one-in-three Americans. Blue Cross and Blue Shield Plans across the country are leaders in advancing health information technology, giving providers and consumers tools and information to help them make better health care decisions. Plans are sharing clinically relevant claims information with physicians; giving consumers access to their medical information through personal health records and other internet-based tools; and helping providers adopt health IT, including e-prescribing and electronic health records (EHRs).

BCBSA is committed to a health care system that can assure greater patient safety, improved quality of care and increased efficiency. We believe that achieving this goal requires nationwide adoption of health IT based on interoperability standards that support the exchange of information among providers, payers, consumers and government. That is why we strongly support the requirement in H.R. 4157 to establish interoperability standards through a public-private collaborative process.

However, we are concerned that the provision calling for switching from ICD-9 to ICD-10 billing codes by October 1, 2009 would threaten the goal of widespread adoption of health IT. Switching to ICD-10 by 2009 is unworkable because:

- ICD-10 is a massive undertaking, not only for payers and hospitals but also for physicians;
- Industry is running at maximum capacity with HIPAA mandates;
- Much preliminary work is needed to make the switch feasible; and
- Medicare would be put at great risk.

Our testimony below will explain these factors, and offer as an alternative three additional years to switch to ICD-10, with full compliance no sooner than October 1, 2012.

In addition, we would like to draw the Committee's attention to a specific issue concerning the provision creating new safe harbors under the federal anti-fraud and anti-kickback laws: the prohibition on taking into account the volume or value of referrals by entities donating health IT to physician. As explained below, this prohibition would have a chilling effect on donations of health IT that are already taking place today.

Switching to ICD-10 by 2009 is Unworkable

In 2003, the Robert E. Nolan Company – a respected business consulting firm – estimated that implementing ICD-10 would cost providers and payers up to $14 billion. This cost is indicative of the complexities involved in switching from ICD-9 to ICD-10.

Provider and Payer Systems will require a Massive Overhaul

ICD codes are ubiquitous in health care. Providers process and store diagnosis and procedure codes in virtually every one of their computer systems, many of which are linked to share information. Payers use diagnosis and procedure codes not only to process claims, but also to design benefit packages, construct fee schedules, operate disease management and quality improvement programs, make medical necessity determinations, and prevent fraud and abuse.

The new ICD-10 coding systems are significantly more complicated than ICD-9. ICD-9-CM (volumes 1 & 2) uses about 13,000 codes for diagnoses; ICD-10-CM uses

120,000 codes for diagnoses. ICD-9-CM (volume 3) uses about 11,000 codes for procedures; ICD-10-PCS uses 87,000 codes for procedures.

To handle these new ICD-10 codes, provider and payer systems must be completely redesigned: field sizes will have to be expanded, alphanumeric composition allowed, and code values and their interpretation completely redefined. IT staff will have to install new code sets, remap and testing every interface used with vendor software (front-end and back-end) and modify all reports used by providers and payers in clinical, financial, reimbursement and quality analyses.

Such far-reaching changes demand adequate time to avoid costly mistakes and disruptions in claims payments.

Physician Practices will Require a Massive Overhaul

If the advantages of the new coding system are to be realized, physicians will need to become substantially more precise and detailed in documenting patients' medical records. To make sure they get the right information from patients to assure proper coding, physicians will need to know ahead of time all of the information that will be required to code according to the new standard – an impossible task without new electronic decision support systems that take physicians through the "decision tree" for each possible diagnosis. Unfortunately, fewer than 15% of physicians currently have electronic health records systems that could be modified to provide such decision support. A report published last year in the *Annals of Internal Medicine* projects on the basis of current trends that in five years' time only 25% of physicians in solo or small group practices will have electronic health records.

Once they gather the needed information, physicians will need to put additional time and effort into documenting patients' medical records, and completing what is sure to become a greatly expanded "superbill" to assure proper reimbursement. In turn, the physician's coders will need to increase their medical knowledge, and the medical staff will need to be aware of the challenges to the physicians and be prepared for greater interaction between the coding staff and the physicians.

Industry is Already at Maximum Capacity with HIPAA

Implementing ICD-10 by 2009 would cause system overload. Payers and providers are currently working hard to implement pending and planned HIPAA tasks. These need to be completed or well underway before implementing ICD-10 because they require the same staff resources. Providers, payers and vendors will all have resources stretched thin over the next several years.

Currently the health care industry is still working to fully implement all of the initial HIPAA transactions. For payers this work includes trading partner testing and making improvements to the level of response in both the claims status and eligibility response transactions.

Another major task currently underway is implementation of the National Provider Identifier (NPI). This project has proven to be much more difficult than originally contemplated because of the complex relationship between NPIs and legacy identifiers. Crosswalks or maps between the two sets of identifiers need to be developed, and in some extremely complex cases re-contracting may be required. The compliance date for this implementation is May 2007, and will most likely require continued use of support staff for the remainder of that year.

Other HIPAA projects on the horizon include electronic claims attachments, which will probably need to be implemented starting in 2007, implementation of the 5010 version of the current HIPAA transactions, and the National Payer Identifier (which has the potential to become as complex as the National Provider Identifier). Each of these projects individually will require substantial human and capital resources. All of this

work, coupled with the scope and complexity of the move to ICD-10, would severely overload system resources and expose the providers and payers to unnecessary risk.

Much Preliminary Work Is Needed

Important steps must happen before the switch to ICD-10 can begin.

First, industry must move to a new version of HIPAA transactions (5010) because the current (4010) will not work with ICD-10. This change alone is a significant upgrade that will require the two years allowed under HIPAA to analyze, program, test, and implement this more complex version. The "implementation guide" that is part of the new 5010 version shows that thousands of changes will need to be made, from comparatively simple tasks like making a change to a single document, to extremely complex tasks like adding the ICD-10 code list. Only after these changes are made should providers and payers begin implementing ICD-10

H.R. 4157 seeks to hurry the process of implementing version 5010 by eliminating notice and comment rulemaking. This would be a mistake. The notice and comment process is industry's primary opportunity to raise business issues that have broad policy implications. To take claims attachments as an example: the SDO might focus on the business requirements around a specific interaction between trading partners such as an unsolicited claim attachment; but CMS would focus on the larger business/policy issue of whether or not to allow claims attachments.

Only the agency's comment and review process gives industry the opportunity to consider the proposed mandate from an enterprise or industry-wide perspective. We believe that global perspective review is essential for the industry and we strongly believe that global review opportunity must be preserved under any revised system for HIPAA changes.

Second, the government must release automated crosswalks that map ICD-9 and ICD-10 – a complete set is not yet available – and providers, payers, and vendors must analyze and test those crosswalks to minimize problems. If the crosswalks do not work properly, historical data will be lost, resulting in an inability to run incentive ("pay-for-performance") programs and the risk of increased fraud and improper payments.

Any change in the underlying code set for claims will undo years of work on fraud detection and control based in ICD-9 coding. Payers have put logic into place within their systems that enable them to see patterns of utilization (such as multiple surgical procedures, assistant surgeon charges, unbundling, upcoding, appropriateness of care, excluded procedures), draw comparisons among providers, and detect claims that fall outside norms.

All of this logic will have to change – which involves the manual process of rewriting all the validity edits – to detect claims irregularities. Depending on the detail and accuracy of the crosswalks, this could be a significant undertaking. Meanwhile, even a small increase in fraud could pose significant risk in a $1.5 trillion health care system.

Medicare Would Be Put At Great Risk

In the largest contracting change since Medicare's inception, CMS is transitioning more than 50 fiscal intermediary and carrier contracts to 15 Part A/B Medicare Administrative Contractors (MACs) by 2009. This will require multiple claims workloads to move from multiple contractors to a single MAC with new jurisdictional lines. At the same time, CMS will be consolidating Medicare workloads into two data centers, which must be done carefully to avoid service disruptions.

The MAC transition will be made in three cycles of competitive bidding, scheduled for completion by summer, 2009. This is a mammoth undertaking with multiple data systems being transitioned to a single entity. The GAO has noted that this massive consolidation in itself has the potential to cause major service problems for Medicare, and the schedule allows little time for CMS to make adjust for any problems.

Switching to ICD-10 by 2009 would further overwhelm Medicare contractors' IT departments, leading to claims backlogs, improper payments, increased opportunities for fraud, and provider and beneficiary dissatisfaction.

BCBSA Recommendation

As switching to ICD-10 by 2009 is unworkable, BCBSA recommends a minimum of three additional years, with compliance no sooner than October 2012. An additional three years would reduce the risk of HIPAA overload and Medicare meltdown, and would provide time for the adoption of decision support systems and significant training and education that physicians and other health care professionals will need.

Pilot Testing

An additional three years would also provide time for pilot testing, which BCBSA believes is critical for any major systems' change. Adequate pilot testing is crucial to ensure the new system works, providers are educated, and claims will be paid: A key lesson from HIPAA is the importance of pilot testing to avoid costly mistakes and assure smooth implementation. ICD-10 is vastly different from the current billing system, with more than 200,000 codes (compared to 24,000 now). The World Health Organization (WHO) also recommends this essential step: "Before starting full-scale countrywide use of ICD-10, it is advisable to test adapted data registration tools and procedures in a number of pilot areas and hospitals. It will help early identification of outstanding problems and fix these before the countrywide implementation starts."

Once comprehensive, automated crosswalks are released, ICD-10 should be pilot tested. Providers and payers would then be able to adjust their systems, and develop a coordinated implementation strategy based on the pilot results. CMS could then set a compliance date that allows the industry to complete the needed adjustments.

Safe Harbors and Limits on Volume

H.R. 4157 stipulates that in order for non-monetary remuneration (in the form of health information technology and related training services for a physician) to fall within the safe harbor, the entity offering the remuneration must not take into account the volume or value of referrals (or other business generated) by the physician to the entity. The problem with this provision is that it would have a chilling effect on donations that are already taking place today by health plans.

For example, it is increasingly common for health plans to promote electronic prescribing by donating e-prescribing hardware and software to physicians. To optimize the allocation of scarce resources, the donation programs commonly target physicians on the basis of volume of prescriptions written or the value of the drugs prescribed. By taking into account volume and value, health plan donations have the most impact on improving physician prescribing habits and improving services provided to the greatest number of health plan members.

Unlike hospitals and group practices, health plans as private payers actively seek to control the fraud and abuse activity the legislation seeks to address—it is a business imperative. As partners with the government on Medicare and Medicaid, health plans are designed to, and have every financial incentive to control utilization costs to compete effectively—the incentives of plans and of the government are aligned by the contractual arrangements to promote gains in efficiency and quality, and to control fraud and abuse.

BCBSA Recommendation

BCBSA recommends that the legislation specifically allow health plans to determine eligibility or the amount or nature of the items and services in a manner that takes into account the volume or value of referral or other business generated between the physician and the health plan.

Conclusion

A minimum of three additional years is critical to switch to ICD-10 – with full compliance by no sooner than 2012 – not only to avoid costly missteps in transitioning from ICD-9 to ICD-10, but also to avoid derailing important health IT initiatives to improve safety, quality, and efficiency. Health IT innovations are exploding as providers and payers devote significant resources to advancing the national priority of widespread adoption of interoperable electronic health records (EHRs) and personal health records (PHRs). For example, many Blue Cross and Blue Shield Plans are building payer-based EHRs and PHRs using claims data and developing regional networks for exchanging administrative and clinical information. Having to redirect resources for an immediate switch to ICD-10 could hinder initiatives promising direct consumer benefit.

SUBMISSION FOR THE RECORD BY DEBORAH C. PEEL, MD, FOUNDER, PATIENT PRIVACY RIGHTS FOUNDATION

Chairman Deal and Members:

The Committee on Health deserves thanks for holding hearings to examine legislative proposals to build a national health Information technology network.

I appreciate the opportunity to provide written testimony on this matter of critical importance, not only to the future of our healthcare system but also to the future of our Democracy and our cherished rights to personal liberty and freedom.

H.R. 4157, the "Health Information Technology and Promotion Act of 2005" promotes the adoption of information technologies to streamline and improve the healthcare system, but at the expense of Americans' most cherished values: personal liberty and privacy.

What is Privacy?

What exactly does it mean to have the right to privacy? The Original Privacy Rule states, "The right of privacy is: 'the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated'." 65 Fed. Reg. at 82,465

The two key reasons HR 4157 and the other HIT bills (with the exception of HR 2234) will eliminate every American's right to privacy are:

1) HR 4157 relies on the HIPAA Privacy Rule as a privacy standard. But the Amended Privacy Rule deprives all Americans of the right of consent, thereby depriving them of the right to control access to their medical records. [citation: *"The **consent provisions…are replaced** with a new provision…that provides regulatory permission for covered entities to use and disclose protected health information for treatment, payment, healthcare operations." 67 Fed. Reg. at 53,211*]
2) HR 4157 sets up a process to study and eliminate all stronger state laws protecting medical privacy. Setting up a process to eliminate more privacy-protective state laws in the absence of a very high national standard set by Congress is a mistake. States' rights to determine how best to protect citizens must not be eliminated without a strong national standard in place.

These two elements of HR 4157 will create a national electronic health system with open access to the nation's medical records by over 800,000 private individuals, corporations, and government agencies; and eliminate states' rights to retain privacy protections stronger than HIPAA.

Other aspects of the bill can be negotiated, but privacy rights cannot. Privacy must be the lynchpin of any system for storing and sharing the nation's medical records.

Consequences of Building a National Health IT System Without Privacy

Without privacy, HR 4157 will have damaging effects that reach far beyond the healthcare system by making electronic medical records instantly accessible for business uses that have nothing to do with healthcare. Broad dissemination of the nation's medical records to hundreds of thousands of covered entities will facilitate discrimination against every man, woman, and child. HR 4157 will enable electronic access to a mother lode of the most commercially valuable databases on earth: the nation's medical databases.

Armed with detailed medical records, private businesses and government agencies will be tempted to discriminate against people based on fears about their future health, rather give them opportunities based on their qualifications and abilities. Will we get jobs, promotions, or bank loans?

Our children's opportunities and livelihoods will be more severely limited than ours, as opportunities will be denied to them earlier in their lives. Will our children and grandchildren get into colleges, get jobs, or be able to buy their first homes?

As the health care system increasingly becomes the province of big business and government, threats to patient privacy will increase exponentially. The immense commercial value of identifiable medical records explains why corporations and the government want unfettered access to everyone's medical records. Privacy (the right to control personal health information) is an important substantive limit on the power of the government and the power of corporations; it limits what they can do.

HR 4157 without privacy is a prescription for disaster.

Introduction

My name is Deborah C. Peel, MD. I have been practicing medicine for 32 years. My specialty is adult psychiatry and Freudian psychoanalysis. My career as a mental health professional put me at ground zero for privacy.

No one would tell me anything if their treatment could be used to harm them. People paid me cash long before managed care or computers were invented, in order to assure their privacy.

Mental health treatment requires the most stringent privacy protections so people will trust mental health professionals with their most painful and terrifying thoughts, feelings, and memories. Patients need privacy and the trust it engenders to speak freely and fully. Mental health professionals need privacy to offer effective psychotherapy, just as surgeons need sterile fields to operate.

I've seen so many people be harmed over the past 32 years when their medical or prescription records were disclosed without their consent.

Without privacy, people will refuse to get treatment and the help they need when they are sick. They will lie and omit data, and refuse genetic and other tests and treatments that could stigmatize them. People will risk worsening illness and even death, rather than risk losing their jobs or reputations.

As a physician, mother, patient, and consumer, I could not stand idly by and watch the destruction of our privacy rights.

No national medical privacy watchdog organization dedicated to fighting to save our rights to privacy existed, so I started Patient Privacy Rights Foundation about three years ago. Our mission is to inform and empower Americans to save their human and civil rights to medical privacy.

Consequences: What happens when patients can't control access to their medical records

1) Diane O'Leary (permission was granted to tell her story). Ms O'Leary is a journalist by profession, living in NY. She developed a rare neurological condition. After the first neurologist she sought treatment from did not help her and the medications he prescribed made her worse, she stopped going to him and sought care elsewhere. But the doctor she fired sent her medical records with his opinions to the new specialists she consulted, without her knowledge or permission. He claimed the HIPAA Privacy Rule gave him the right to disclose her medical records. The disclosures effectively kept her from getting the correct diagnosis and treatment for three years. She was partially disabled and can no longer work as a journalist.

2) Patricia Galvin (permission was granted to tell her story). Ms Galvin is a lawyer who was being seen in a sleep disorders clinic at Stanford University. She saw a therapist in the clinic who repeatedly assured her that the

handwritten records she kept of their therapy sessions would not be entered into Ms Galvin's general medical record. But they were. Once her therapy records were scanned and placed in her general medical record, Ms Galvin could not prevent the records from being repeatedly disclosed by the hospital without her permission, because HIPAA allows disclosures of medical records for all routine uses. Her medical records were sent to her insurer and employer, who fired her and because of some errors in the records and she also lost her disability coverage for an unrelated back injury.

3) A physician whistleblower wrote Patient Privacy Rights about his concerns that the VA's electronic medical records system allows anyone with access to the system to see any patient's medical records without the patient's knowledge or permission (permission was granted to share his story). He gave 3 examples of very sensitive records that VA staff could view:
    - a man had a device inserted into his penis, the nursing notes described the time, length, and size of his erection
    - a woman suffering from painful intercourse had detailed chart notes about the depth and timing of her partner's vaginal penetration to remedy her symptoms
    - an x-ray technician who took a shoulder x-ray of a man had read his mental health notes and asked him if he was still suicidal. The man went to the VA psychiatrist and fired her and refused further treatment

4) Parents of children diagnosed with autism expressed outrage that the CDC was obtaining their children's medical records and school records without notice or consent, a use the HIPAA Privacy Rule makes fully legal for covered entities. [National Autism Association Press Release - 3/1/2006 - CDC Obtains Children's Confidential Records Without Parental Consent For Autism Study]

5) A college student was expelled from GWU because his medical records concerning his depression were disclosed to the college without his consent. [GWU Suit Prompts Questions Of Student Liability; School Barred Depressed Student, Washington Post - 3/10/2002]

6) Insurers now ask doctors to disclose patients' complete medical records, using HIPAA to justify access without patient consent:

   Email from Robert Charles Powell, MD, PhD on 3/11/06 to a psychiatric listserv (permission was granted to share the email for testimony): "Now that HIPAA is attempting to be lord of the land, there are more and more requests for "all medical records and notes" -- which is an illegal request of a psychiatrist under the Illinois Confidentiality Act. I don't know how this ultimately will shake out, but it is worth noting that the Ohio Supreme Court recently upheld that state's confidentiality act -- almost as good as Illinois' -- noting (a) that the state act offered the patient more protection than HIPAA and therefore should be followed plus (b) that the physician had a responsibility to protect the patient's privacy regardless of whatever piece of paper the patient might have signed [the Illinois act specifies likewise that a patient can NOT sign away protected confidentiality rights. [Grove v. Northeast Ohio Nephrology Associates (Ohio Ct. App., Nos. 22594, 22585, 12/26/2005)]

7) Wal-Mart:

Quotes from the Memorandum to Wal-Mart's Board of Directors:

- "Redesign benefits and other aspects of the Associate experience, such as job design, to attract a healthier, more productive workforce."
- "The team is also considering additional initiatives to support this objective, including: all jobs to include some physical activity (e.g., all cashiers do some cart gathering)."

See New York Times story October 26, 2005: Wal-Mart Memo Suggests Ways to Cut Employee Benefit Costs, By Steven Greenhouse and Michael Barbaro.

[Supplemental Benefits Documentation, Board of Directors Retreat FY06, Wal-Mart Stores, Inc., Reviewing and Revising Wal-Mart's Benefits Strategy, Memorandum to the Board of Directors, http://www.patientprivacyrights.org/site/DocServer/WalMart_memo.pdf?docID=501]

8) FDIC Notice on Medical Privacy. This example is included to show how access to medical records is widespread, far beyond the direct uses in the healthcare system. Enough medical records were in the hands of banks and financial institutions for the FDIC to issue a formal memo on April 28, 2004. Furthermore, the Gramm-Leach-Bliley Financial Services Act permits banks and financial institutions to share medical and financial records with all their affiliates and non-affiliates without consumer consent.

The FDIC acknowledges that banks and financial institutions have medical records, "section 411 prohibits creditors from obtaining or using medical information to make credit determinations**.** Except as permitted by the regulators or the FACT Act itself, section 411 treats medical information as a credit report when a creditor shares it with an affiliate." Further, section 411 states that "a creditor may not obtain or use a consumer's medical information, as defined in the Act, in connection with a determination of a consumer's eligibility, or continued eligibility, for credit…**..**section 411 states that when affiliates share certain medical information, that information will be considered a consumer report under the FCRA**."**

9) Patients' medical records can be sent around the world without their knowledge for transcribing, because under HIPAA patients have no right to consent to or even be notified of this "routine" practice.

See San Francisco Chronicle story by David Lazarus: A tough lesson on medical privacy, Pakistani transcriber threatens UCSF over back pay Wednesday, October 22, 2003 URL: sfgate.com/article.cgi?file=/c/a/2003/10/22/MNGCO2FN8G.DTL

10) "Placentas taken, but moms were not told." Susan Goldman of the Oregonian reported on Sunday February 12, 2006, that "as many as 700 afterbirths, many involved in difficult deliveries, made their way to a Portland registry, records show." Not getting consent to analyze women's body parts following births of children with injuries or defects is a severe violation of their privacy.

[http://www.oregonlive.com/search/index.ssf?/base/news/1139707514288820.xml?oregonian?lctop&coll=7]

11) Patients can no longer control who can access their records, so as our medical records are disclosed over and over to people we do not about, our records will be stored in many more locations we have no knowledge of, exposing us to high risk of identity theft because electronic systems are NOT secure.

See: TechWeb News March 9, 2006, by Gregg Keizer: PIN Scandal 'Worst Hack Ever'; Citibank Only The Start "The scam has hit national banks like Bank of America, Wells Fargo, and Washington Mutual, as well as smaller banks, all of which have re-issued debit cards in recent weeks, says a Gartner research vice president." http://www.informationweek.com/story/showArticle.jhtml?articleID=181502474]

12) There is no meaningful recourse or right of action under HIPAA if your privacy is violated. You can only complain to HHS. The woman caught in an FBI sting operation is only the second conviction for a privacy violation since HIPAA took effect. The first was a conviction for identity theft that was later overturned. The second story from TMCNews reported that of the 17,000 complaints of privacy violations made to the government, only one person was prosecuted. 70% were dismissed because they were legally permitted disclosures. Because HIPAA grants legal access to over 800,000 individuals, corporations, and government agencies, patients have no right or opportunity to stop access by any of them.

See Laredo Morning News - 3/7/2006, Alamo Woman Guilty of Selling Medical Information at: http://www.patientprivacyrights.org/site/News2?page=NewsArticle&id=5807&news_iv_ctrl=-1

See also TMCNet News, February 24, 2006 at http://www.tmcnet.com/usubmit/2006/02/24/1404832.htm

Don't Confuse Privacy and Security

It is important not to confuse the privacy with security. Security can help protect medical records from illegal users like hackers, but it cannot restore or substitute for the right to control who can see and use your medical records. The terms are often used interchangeably, confusing their different effects on access to medical records.

Privacy means that patients control who can see and use their electronic medical records, which means they can exclude any individual or corporation from having access to their medical information.

Security measures such as encryption, firewalls, passwords, levels of access, and other physical and technical measures can help protect medical records from illegal access by hackers and identity thieves. But security measures do nothing to stop the over 800,000 covered entities that currently have legal access to medical records from using them. Strong security measures are not a substitute for privacy.

Need for a system of trusted couriers and trusted custodians

The health IT system should be designed and engineered to be a system of trusted couriers and custodians. It should be structured to permit access to medical records only with patient permission (emergencies could be specifically excluded). That is how FedEx

works. We trust FedEx to deliver our packet of information to only the person we specify.

Instead, in the electronic world, any data broker, data warehouse, and any healthcare business that handles, stores or processes medical records simply appropriates them for corporate use. If FedEx operated like that—where anyone who happened to handle the packet of information could tear it open, make copies, and use and sell the data, it would not have any customers.

Surely our sensitive health information should not be accessible to all covered entities to copy and steal just because they happen to be in a business that is connected to the healthcare system.

Conclusions

- Congress should intervene when private actions have such vast public consequences. The failure of Congress to intervene and specify the rights patients should have---the right to control access to their medical records---- will undermine significant Constitutional values and impair important individual privacy rights.
- Congress should set privacy standards, not delegate the task to unelected officials with no Congressional or public input or oversight.
- With ironclad privacy standards and patient privacy rights in place, patients will be willing to trust and use the national electronic health system and the incredible and transforming benefits that IT can bring to the healthcare system will be fully realized.

Solutions to Insure the Privacy Of Medical Records In Electronic Networks and Systems

- Patients must control who has access to their personal health information over any electronic health networks
- Allow patients to opt-in and opt-out of health information networks
- Allow patients to segregate their most sensitive medical records
- Require audit trails of all disclosures
- Require patient notification of all suspected or actual privacy and security breaches
- Deny employer access to employee medical records
- Allow access to de-identified medical records for research, public health, and other legitimate uses
- Preserve stronger state laws protecting medical privacy
- Enact criminal penalties for use or possession of medical records without permission

Deborah C. Peel, MD
Chairman, Patient Privacy Rights Foundation
Austin, Texas
512-732-0033
www.patientprivacyrights.org

SUBMISSION FOR THE RECORD BY ADVANCED MEDICAL TECHNOLOGY ASSOCIATION

AdvaMed and its member companies thank the Committee for holding this hearing on health information technology (HIT). HIT promises to revolutionize the health care delivery system and dramatically effect patient safety, quality of care, and efficiency. HIT products and applications are greatly expanding throughout vital sectors of the American health care delivery system, including clinical operations, decision support, devices, equipment, distribution, administrative tasks, and the interface with payers. As a result, HIT is helping to significantly reduce medical errors, improve the quality of care, speed paperwork, and reduce administrative costs.

AdvaMed is the world's largest medical technology association representing manufacturers of medical devices, diagnostic products and medical information systems. AdvaMed's more than 1,300 members and subsidiaries manufacture nearly 90 percent of the $75 billion of health care technology purchased annually in the United States and more than 50 percent of the $175 billion purchased annually around the world. Many of these technologies – such as electronic infusion pumps that administer intravenous (IV) drugs, verify correct drugs, and check dosages, as well as remote physiological monitoring (RPM) technology – save lives and improve the quality of life for patients by preventing medication errors and managing disease.

The Role of Technology

Universally interoperable electronic health records (EHR) hold great promise in reducing health care costs and improving the quality of care delivered to patients. The Department of Health and Human Services (HHS) cites two studies that estimate savings from implementing EHRs to be between $78 and $112 billion. HIT, however, is expanding far beyond the EHR to include devices that are already dramatically improving patient safety, quality of care, and health care efficiencies. Combined, the EHR and these other innovative technologies will ultimately play a major role in reducing overall health care costs. Examples of these innovations include:

- Computer-assisted physician order entry devices to increase patient safety and health system efficiency;
- Hand-held Personal Digital Assistants (PDAs) to allow doctors making rounds to immediately access each patient's complete medical record;
- Electronic lab results to allow test results to be stored and sent to physicians electronically;
- Electronic prescription orders to allow physicians to send prescriptions directly to pharmacists to ensure accurate order submissions and allow pharmacists to conduct drug interaction reviews;
- Infusion pumps to prevent drug overdoses and enable hospitals to re-engineer their systems to avoid medical errors;
- Image-guided or computer-assisted surgery (CAS) to allow surgeons to more precisely position their instruments for less invasive operations and to document procedures;
- Remote monitoring, telemedicine, and other devices with computerized components, such as implantable cardioverter-defibrillators (ICDs), to allow heart patients to send vital data to their physicians via a secure Internet connection, often reducing trips to the doctor; and
- Picture archiving and communication (PAC) systems to store and permit the transmittal of radiological images, such as X-rays.

Improving Patient Safety and Quality of Care

The Institute of Medicine (IOM) estimates that 44,000 to 98,000 deaths each year result from preventable medical errors in hospitals. Studies have shown that there are errors in 24.9 percent of hospital patient records.[1] An estimate by the Food and Drug Administration (FDA), found that as many as 372,000 preventable adverse drug events occur each year.[2] These errors result from administering incorrect dosages, errors in filling prescriptions, and adverse drug interactions.

Technologies that support IV drug administration can help prevent medication errors using automated dosage limits and alerting systems. Electronic physician ordering systems and data management software reduce transcription and dosing errors, promote process standardization, increase access to patient specific medical information, and reduce laboratory turnaround time.

For example, a report by the National Academies in 2003 recommended that health care organizations adopt information technology systems capable of collecting and sharing health information about patients and their care. Computerized physician order entry (CPOE) devices can link the health care worker with the facility's computer system to avert medical errors. These computerized systems can automatically alert the practitioner to past drug allergies, potential drug interactions with a patient's current medications, and incorrect dosing.

The Children's Hospital of Pittsburgh (Children's) launched its CPOE program, Children's Net, in October 2002. It helps this pediatric hospital with its special challenge with medication errors due to their patients' weights, as well as meeting the regulatory requirements for compliance to reach certain care benchmarks. Children's CPOE system allows doctors to show lab or diagnostic test results to parents at the child's bedside, chart functions, and graph progress. Its warning system provides an alert if a dose seems out of line, based on predetermined standards, and the CPOE has reduced medication errors by 75% and virtually eliminated weight related adverse drug events.

Reducing Costs

By reducing duplicative care, lowering health care administration costs, and avoiding care errors, health information technology could save approximately $140 billion per year, according to HHS. Studies cited by HHS in its 2004 Health IT Strategic Framework Report suggest the use of EHRs can reduce laboratory and radiology test ordering by 9 percent to 14 percent, lower ancillary test charges by up to 8 percent, reduce hospital admissions ($16,000 average cost) by 2 percent, and reduce excess medication usage by 11 percent. Two studies have estimated that ambulatory EHRs have the potential to save all payers $78 billion to $112 billion annually. HHS also cites evidence that EHRs have the potential to reduce administrative inefficiency and paperwork.

A 2004 study in Critical Care Medicine found that using remote Intensivists (intensive care specialists) to monitor patients electronically from a remote location as part of an ICU telemedicine program not only improves clinical outcomes, but also enhances hospital financial revenues.[3] Cost savings resulted both from a reduction in the

---

[1] Terri Simmonds. "Using The Trigger Tool to Detect Potential Harm in Medication Management." Infusion Safety: Addressing Harm with High-Risk Drug Administration. The ALARIS® Center for Medication Safety and Clinical Improvement. San Diego, California. 2004, pp 10.

[2] Steven Tucker. "Analysis of Impact of the Food and Drug Administration's Proposed Bar Code Label Requirements for Human Drug Products and Blood." Hospital Pharmacy. 38 (11), Supplement 1, pp S11.

[3] Breslow MJ, Rosenfeld BA, Doerfler M, Burke G et al. Effect of a multiple-site intensive care unit telemedicine program on clinical and economic outcomes: An alternative paradigm for Intensivist staffing. Crit Care Med 2004;32:31-38.

average length of stay in the ICUs (3.63 days vs. 4.35 days) and from a decrease in daily costs.

In addition, picture archiving and communication systems (PACS) enable hospitals, imaging centers and multi-site health care organizations to manage, store and transmit patient medical images such as digital X-ray, MRI and CR images. Combining this kind of technology with a digital patient information system allowed several Boston-area hospitals to save an estimated $1 million annually by, in part, reducing the time spent searching for files and manually admitting patients.[4]

Policies to Foster HIT Adoption

To assure appropriate access to continued innovations in health information technologies for patients, AdvaMed believes that policies should evolve with the technologies. We support developing incentives that will overcome the barriers to timely adoption HIT. Providers, payers, and medical technology manufacturers should all be involved in developing the ways to address these issues and enable interoperable and efficient use of these technologies to improve the quality of care, patient safety, and health outcomes overall. Specifically, we support the following provisions for inclusion in HIT legislation:

Regulatory Reforms: The implementation of the International Classification of Diseases, version 10 (ICD-10) will have an impact on the timely adoption of life-saving and life-enhancing medical technology. ICD-10 is the next generation of the coding system that will modernize and expand CMS's capacity to keep pace with changes in medical practice and technology. Its unique structure will incorporate all new procedures as unique codes that would explicitly identify the technology used to perform the procedure. The transition from the currently used ICD-9 system to the internationally used ICD-10 system is time-sensitive as the number of available codes under ICD-9 is rapidly dwindling. The availability of new codes has been raised in public meetings as a potential basis for CMS to deny applications for new codes, and this reluctance to issue new codes will hinder appropriate tracking, identification, and analysis of new medical services and technologies.

In 2003, after several years of hearings, the National Committee of Vital and Health Statistics (NCVHS) raised concerns about the viability of the ICD-9-CM as it was "increasingly unable to address the needs for accurate data for health care billing, quality assurance, public health reporting, and health services research." NCVHS also noted in 2003 that these concerns have been "well documented" in the testimony and letters provided to the NCVHS over the past several years. HHS has yet to begin this important transition.

Without adoption of ICD-10, it will be difficult to track new and emerging public health threats, such as avian flu. ICD-10 is also the key to collecting the information needed to implement a proper pay-for-performance system for providers and carry out Medicare's road map for the future, which depends on accurate data on the effectiveness of treatments. ICD-10 will also enable better patient care through better understanding of the value of new procedures, improved disease management, better understanding of patients' health care outcomes, and an improved ability to study patient outcomes.

While concerns have been raised about the cost of implementing ICD-10, we note that the 2004 RAND study found that the financial benefits of ICD-10 significantly outweigh the costs, and the study did not even account for the significant costs that will accrue for not adopting the system in a timely fashion. Additionally, several cost estimates that have been circulated to attempt to dissuade support for ICD-10 are flawed

---

[4] Networking Health: Prescriptions for the Internet, Institute of Medicine, National Academy of Sciences, p. 81, 2000.

by failing to net out costs of the normal upgrading of all payment systems that would occur independent of ICD-10.

We believe that the long term and ongoing benefits of improved measurements of efficiency, complications, resource use, and improved accuracy of payments would more than offset the one-time or short-term costs of the conversion to ICD-10.

Some existing laws and regulations present barriers to the adoption of HIT. Currently, unless an exception is met, provisions of the federal health care program anti-kickback statute prohibit the offer or acceptance of anything of value in return for patient or item/service referrals. Likewise, unless an exception is met, the physician self-referral law (the "Stark" law) bars hospitals from billing for items or services provided by physicians who have financial relationships with the hospital. While an exception to Stark has been promulgated by the Centers for Medicare and Medicaid Services for community-wide health information systems, the exception is not well defined or understood, and a much broader, clearer exception is needed.

A parallel safe harbor to the federal health care program anti-kickback statute is also necessary. These barriers to the dissemination of resources (financial, equipment or otherwise), such as a hospital financially supporting its referring physicians in the acquisition and use of health information technology, must be removed. While the proposed EHR and e-prescribing exceptions to both the anti-kickback and Stark laws are an important step in the right direction, they do not go far enough to protect the adoption of HIT.

In addition, AdvaMed is concerned with the impact of an increasing array of state and local laws on interoperable health systems that resulted from the enactment of the Health Insurance Portability and Accountability Act (HIPAA). Our member companies operate in a multi-state, multi-jurisdictional environment, and the overlapping multiplicity of these laws makes it costly and complex to develop compliant processes and systems for protecting confidentiality and securing information. AdvaMed believes that uniform federal standards for privacy, security, and technical regulations are critical to achieving a nationwide electronic health information exchange, and the lack of uniform federal standards should not delay this effort.

Standards: AdvaMed endorses the FDA's current software regulation policies, under which it only regulates software if its output directly results in software-directed treatment or diagnosis of patients. We also believe that the FDA's regulation of any software associated with medical devices should be risk-based and only at the minimum level necessary to protect public health. Since the EHR is not a medical device and simply stores data for retrieval by a health care professional (EHR algorithms do not make diagnostic or treatment decisions), FDA regulation is not warranted for EHRs under the FDA's own standards.

Financial Incentives: Many providers lack the financial ability to make the upfront investment needed to install and operate an advanced health information technology system. The federal government and other payers should provide financial incentives sufficient to spur widespread, rapid adoption of health information technology throughout the health care system, including universal adoption of EHRs. "Pay-for-performance" proposals should include incentives for adoption and use of HIT.

Direct Reimbursement: Reimbursement systems should reward new modes of providing services that result in quality improvement or cost reduction for patient care. Remote patient management of chronic diseases is one example of a quality-enhancing technology for which health care practitioners are not directly reimbursed under Medicare. Many Medicare beneficiaries living in rural or underserved urban areas are unable to make regular visits to their physicians. As a result, patients with treatable chronic diseases such as diabetes, cardiac arrhythmia, and heart failure do not receive the care they require to manage their conditions.

Remote patient management would ensure that Medicare beneficiaries would have access to real-time disease management services for covered chronic conditions. Direct reimbursement to health care practitioners for utilization of remote patient monitoring devices would facilitate use of this technology and lead to improved patient outcomes. AdvaMed also supports providing physicians with a quality-of-care incentive bonus for meeting specific standards of care for covered chronic diseases.

Quality and Safety Studies: The e-health system should be designed to assure that data from the electronic medical record would be available, with appropriate privacy protections under HIPAA, for studies to improve patient safety, and quality of care.

Conclusion

Again, we thank the Committee for holding this hearing today. HIT holds great promise for improving patient safety, improving the quality of medical care, and increasing efficiency. While EHR is one of the many medical devices that can attain this goal, HIT is expanding far beyond this and dramatically improving patient safety, quality of care, and health care efficiencies.

Despite the existing and growing body of evidence that HIT will improve patient safety, enhance the quality of care, and increase efficiency of care provided, many barriers to adoption remain. We urge expeditious implementation by CMS of the ICD-10 system and federal preemption of HIPAA rules to ensure that data may be stored, updated, and transmitted electronically anywhere in the United States. Legislation is needed to address the regulatory barriers to HIT adoption, like the federal health care program anti-kickback statute and the "Stark" physician self-referral law. As clinical and interoperability standards are developed by Congress and the private sector, it is paramount that the standards are designed to evolve with advancements in technologies and that financial incentives are provided to allow providers to purchase and maintain the HIT.

○