AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 110–114

PRIVATE HEALTH RECORDS: PRIVACY IMPLICATIONS OF THE FEDERAL GOVERNMENT'S HEALTH INFORMATION TECHNOLOGY INITIATIVE

HEARING

BEFORE THE

OVERSIGHT OF GOVERNMENT MANAGEMENT, THE FEDERAL WORKFORCE, AND THE DISTRICT OF COLUMBIA SUBCOMMITTEE

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

FEBRUARY 1, 2007

Available via http://www.access.gpo.gov/congress/senate

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

33–874 PDF WASHINGTON : 2007

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 HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
BARACK OBAMA, Illinois
CLAIRE McCASKILL, Missouri
JON TESTER, Montana

SUSAN M. COLLINS, Maine
TED STEVENS, Alaska
GEORGE V. VOINOVICH, Ohio
NORM COLEMAN, Minnesota
TOM COBURN, Oklahoma
PETE V. DOMENICI, New Mexico
JOHN WARNER, Virginia
JOHN E. SUNUNU, New Hampshire

MICHAEL L. ALEXANDER, *Staff Director*
BRANDON L. MILHORN, *Minority Staff Director and Chief Counsel*
TRINA DRIESSNACK TYRER, *Chief Clerk*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, THE FEDERAL WORKFORCE, AND THE DISTRICT OF COLUMBIA

DANIEL K. AKAKA, Hawaii, *Chairman*

CARL LEVIN, Michigan
THOMAS R. CARPER, Delaware
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana

GEORGE V. VOINOVICH, Ohio
TED STEVENS, Alaska
TOM COBURN, Oklahoma
JOHN WARNER, Virginia

RICHARD J. KESSLER, *Staff Director*
JENNIFER A. HEMINGWAY, *Minority Staff Director*
EMILY MARTHALER, *Chief Clerk*

CONTENTS

	Page
Opening statements:	
Senator Akaka	1
Senator Voinovich	3
Senator Carper	4

WITNESSES

THURSDAY, FEBRUARY 1, 2007

Robert Kolodner, M.D., Interim National Coordinator for Health Information Technology, U.S. Department of Health and Human Services	5
Daniel A. Green, Deputy Associate Director, Center for Employee and Family Support Policy, Office of Personnel Management	7
David A. Powner, Director of Information Technology Management Issues, Government Accountability Office, accompanied by Linda Koontz, Director of Information Management Issues, Government Accountability Office	17
Mark A. Rothstein, Herbert F. Boehl Chair of Law and Medicine, and Director, Institute for Bioethics, Health Policy and Law, University of Louisville School of Medicine	19
Carol C. Diamond, M.D., Managing Director, Markle Foundation, and Chair, Connecting for Health	20

ALPHABETICAL LIST OF WITNESSES

Diamond, Carol C., M.D.:	
Testimony	20
Prepared statement with attachments	138
Green, Daniel A.:	
Testimony	7
Prepared statement	44
Kolodner, Robert, M.D.:	
Testimony	5
Prepared statement	35
Koontz, Linda:	
Testimony	17
Prepared statement with attachments	52
Powner, David A.:	
Testimony	17
Prepared statement with attachments	52
Rothstein, Mark A.:	
Testimony	19
Prepared statement	130

APPENDIX

Background Memorandum	29
Simon P. Cohn, M.D., M.P.H., Chairman, National Committee on Vital and Health Statistics, submitted copy of a report entitled "Privacy and Confidentiality in the Nationwide Health Information Network"	164
Response to questions submitted for the Record from:	
Dr. Kolodner	181
Mr. Green	185
Mr. Powner	188

PRIVATE HEALTH RECORDS: PRIVACY IMPLICATIONS OF THE FEDERAL GOVERNMENT'S HEALTH INFORMATION TECHNOLOGY INITIATIVE

THURSDAY, FEBRUARY 1, 2007

U.S. SENATE,
SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT
MANAGEMENT, THE FEDERAL WORKFORCE,
AND THE DISTRICT OF COLUMBIA,
OF THE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:33 p.m., in room SD–342, Dirksen Senate Office Building, Hon. Daniel K. Akaka, Chairman of the Subcommittee, presiding.

Present: Senators Akaka, Carper, and Voinovich.

OPENING STATEMENT OF CHAIRMAN AKAKA

Chairman AKAKA. This hearing will come to order.

Today's hearing, "Private Health Records: Privacy Implications of the Federal Government's Health Information Technology Initiative," will examine what actions the Federal Government is taking to ensure that privacy is an integral part of the national strategy to promote health information technology.

Studies show that the use of health IT can save money, reduce medical errors, and improve the delivery of health services. For example, in 2004, the Center for Information Technology Leadership estimated that in ambulatory care settings the use of electronic health records (EHRs) would save $112 billion per year, or 7.5 percent of health care spending. In addition, EHRs are shown to help avoid duplicate tests and excess medication.

In 2004, President Bush called for the widespread adoption of interoperable electronic health records within 10 years and issued an Executive Order that established the position of the National Coordinator for Health Information Technology. The National Coordinator is charged with developing and implementing a strategic plan to guide the nationwide implementation of interoperable health IT in both the public and private sectors.

Two months later, the Department of Health and Human Services (HHS) released a framework for strategic action to promote health IT, which calls on all levels of government to work with the private sector to stimulate change in the health care industry. For example, the Departments of Veterans Affairs (VA) and Defense

(DOD), the major Federal health care delivery organizations, are leaders in the use of health IT.

VA, one of the country's largest health care providers, has had an automated information system in its medical facilities since 1985. DOD has provided IT support to its hospitals and clinics since 1968. As Chairman of the Veterans' Affairs Committee, we are looking at how to move DOD and VA forward in developing joint EHRs.

This Subcommittee is particularly interested in the strategy, which calls for the Office of Personnel Management (OPM) to use its leverage as the administrator of the Federal Employee Health Benefits Program, which covers approximately 8 million Federal employees, retirees, and their dependents, to expand the use of health IT. OPM, through its annual Call Letter to carriers, has been encouraging carriers to increase the use of EHRs, electronic prescribing, and other health IT-related provisions.

Although I support efforts to increase the use of health IT, I am deeply concerned about the level of privacy protections in the health IT network. In 2005, a Harris Interactive survey showed that 70 percent of Americans were concerned that an electronic medical records system would lead to sensitive medical records being exposed due to weak electronic security. This fear is understandable.

Over the past few years, we have seen various data mining programs in the Federal Government that lacked key privacy protections. We also recall the loss of a VA laptop computer and the news of many other Federal data breaches that put the personal information of millions of Americans at risk. These incidents reinforce the need to build privacy and security protections into any system containing personal information. Our personal health information must not be subject to these same failings. Privacy and security are critical elements in health IT and should never be an afterthought.

That is why I wrote to OPM in May 2005 seeking information on how Federal employees' health information would be protected under the efforts of OPM and the health insurance carriers. OPM responded that the Health Insurance Portability and Accountability Act (HIPAA) would address these privacy concerns. But while HIPAA is a foundation, HIPAA by itself is not enough. Privacy protections must be built in conjunction with the development of the health IT infrastructure.

To ensure that this was happening, Senator Kennedy and I asked the Government Accountability Office to review the efforts of HHS and the National Coordinator to protect personal health information. GAO's report, which was released this morning, found that while HHS and the National Coordinator have taken steps to study the protection of personal health information, an overall strategy is needed to: One, identify milestones for integrating privacy into the health IT framework; two, ensure privacy is fully addressed; and, three, address key challenges associated with the nationwide exchange of information.

Given the overwhelming evidence of the benefits associated with the expanded use of health IT, as well as the fact that 70 percent of Americans are concerned about the privacy of their health infor-

mation, I am surprised to learn that HHS objects to this recommendation.

It is clear that the health care industry faces challenges in protecting electronic health information given the varying State laws and policies, the entities not covered by HIPAA, and the need to implement adequate security measures. But while more and more companies, providers, and carriers move forward with health IT, I fear that privacy suffers while HHS takes time to decide how to implement privacy protection. HHS must address these issues in a more timely fashion in order to give the private sector guidance on how to move forward with health IT and protect the private health information of all Americans.

I want to thank our witnesses for being here today to discuss this critical issue.

I now turn to my good friend, Senator Voinovich, for any opening statement he may have at this time.

OPENING STATEMENT OF SENATOR VOINOVICH

Senator VOINOVICH. Thank you, Senator Akaka. I appreciate your holding this hearing today on a subject that is of interest to me.

The widespread adoption of health information technology such as electronic health records will revolutionize the health care profession. In fact, the Institute of Medicine, the National Committee on Vital and Health Statistics, and other expert panels have identified information technology as one of the most powerful tools in reducing medical errors and improving the quality of health.

Unfortunately, our country's health care industry lags far behind other sectors of the economy in its investment in information technology. But, Senator Akaka and Carper, as I travel around Ohio I see a marked acceleration in the use of IT.

The Institute of Medicine estimated in 1999 that there were nearly 98,000 deaths each year resulting from medical errors. Many of these deaths can be directly attributed to the inherent imperfections of our current paper-based health care system.

Not only can technology save lives and improve the quality of health care, it also has the potential to reduce the cost of the delivery of health care. According to the Rand Corporation, the health care delivery system in the United States could save approximately $160 billion annually with the widespread use of electronic medical records. As technology advances, the issues surrounding protection of personal information will continue to be at the forefront of people's minds. Individual citizens continue to express concern over the security of personal, confidential information whether it is contained in an electronic health record or stolen from laptops, as Senator Akaka pointed out, at the Department of Veterans Affairs.

However, the benefits of technology in the health care arena are undeniable, and I support the use of HIT. In fact, in the 109th Congress, Senator Carper and I introduced the Federal Employees Electronic Personal Health Records Act. I am sure we will be hearing more from Senator Carper about it. The bill will provide for the establishment and maintenance of electronic personal health records for individuals and family members enrolled in the Federal

Employee Health Benefits Program. I have talked with one of the major health insurance companies and they support the use of HIT.

I am hopeful the testimony today will assist my colleagues and me as we make decisions about implementing health IT. I personally look forward to learning from our witnesses ways Senator Carper and I might refine our legislation before introduction. As I say, we are making progress on privacy protections, and I am really pleased that the President issued an Executive Order specific to deployment of health information technology, including establishment of a National Coordinator for Health Information Technology.

Since then, the Coordinator and the Department of Health and Human Services have made considerable progress toward the adoption of interoperable IT. But the successes have not come without criticism. Dr. Kolodner, your office has an enormous responsibility to continue to cultivate a strategic plan to guide implementation of nationwide interoperable health information technology. It is an important job. We must bring health care costs under control, and HIT is one part of that goal. However, there is some concern about whether information in IT systems is going to be private and secure. We cannot let those weaknesses impede our progress in this area.

So, Mr. Chairman, I am looking forward to hearing from our witnesses.

Chairman AKAKA. Thank you very much, Senator Voinovich. Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thank you, Mr. Chairman, and to our witnesses and to my friend and colleague, Senator Voinovich. He telegraphed my pitch a little bit, but I think it is great that he did.

Mr. Chairman, as Senator Voinovich has said, we introduced in the last Congress and I think we are close to reintroducing in this Congress legislation to require those who provide insurance under the Federal Employee Health Benefits Program—they would have a period of time, I think maybe less than 2 years or so—to provide electronic health records for Federal employees insured under those policies if the employees wish to have that. And I know you have a strong interest in privacy protection, and we would look forward to working with you and your Subcommittee and your staff to make sure that we meet muster in that regard.

Next month is a big month for us in Delaware, and I say this to our witnesses and others. We are beginning to stand up what we call the "Delaware Health Information Network," an apple in my eye when I was Governor many years ago, and it is now actually coming to fruition as we try to electronically link our doctors' and nurses' offices and our hospitals and our labs and other providers. We are excited about the possibilities that holds for us.

I am an old Navy guy, and I remember when I got out of the Navy—at least off of active duty, not out of the Navy, but off of active duty in 1973 and showed up at the VA hospital just outside of Wilmington. And it is not a place that, frankly, a lot of veterans wanted to go to for health care. I did not sense there was a lot of joy on the part of people who worked there being a VA employee,

doctor or nurse or anything else. And, boy, that has really changed, especially in the last decade.

I would never have imagined 33 years ago, that we would be looking to the VA to provide the way with respect to improving outcomes and holding down costs and saving lives. But they sure have come through for us.

Mr. Chairman, don't you chair the Veterans Committee in the Senate?

Chairman AKAKA. Yes.

Senator CARPER. I thought so. OK. Well, you have sort of a double interest in this particular issue. But we really look forward to what you have to say. We do not have very strong attendance here today, partly because there is a concurrent just-called caucus of the Senate Democrats, and they are meeting as we speak to discuss a resolution that pertains to the President's proposed surge of troops in Iraq. So people may be drifting in to join us in a little bit, but that just began literally at the time that this hearing began. So we apologize for them. Those of us who are here are anxious to hear what you have to say. So thanks for coming.

Chairman AKAKA. Thank you very much.

I welcome to the Subcommittee today's first panel of witnesses: Dr. Rob Kolodner, Interim National Coordinator for Health Information Technology at the Department of Health and Human Services, and Daniel Green, Deputy Associate Director, Center for Employee and Family Support Policy, at the Office of Personnel Management.

It is the custom of this Subcommittee to swear in all witnesses, and I ask you to stand and raise your right hand. Do you swear that the testimony you are about to give this Subcommittee is the truth, the whole truth, and nothing but the truth, so help you, God?

Dr. KOLODNER. I do.

Mr. GREEN. I do.

Chairman AKAKA. Thank you. Dr. Kolodner, please proceed with your statement.

TESTIMONY OF ROBERT KOLODNER, M.D.,[1] INTERIM NATIONAL COORDINATOR FOR HEALTH INFORMATION TECHNOLOGY, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Dr. KOLODNER. Good afternoon, Chairman Akaka, Senator Voinovich, and Senator Carper. Thank you for inviting me here today to discuss the privacy plans, activities, and accomplishments of the National Health Information Technology agenda led by HHS.

Mr. Chairman, we appreciate Hawaii's efforts as pioneers in protecting patient health information and note that Hawaii's early work to develop a comprehensive privacy law informed and was an important resource for HHS when we developed the HIPAA privacy rules.

Privacy and security are integral components of the national health IT agenda and are addressed by a spectrum of activities that advance our current understanding of the issues and multiple

[1] The prepared statement of Dr. Kolodner appears in the Appendix on page 35.

levels and lay the foundation for future activities. The widespread adoption of interoperable electronic health records will save lives, reduce medical errors, and improve the quality and efficiency of care, as you have noted.

At the same time, it will create both new challenges and new opportunities with respect to protecting health information. HIPAA created a strong foundation of privacy and security protections for personal health information upon which States may provide additional privacy protections. We are vigorously addressing the new challenges by leveraging existing privacy policy foundations, building robust new public-private collaborations, partnering with States, health care organizations, and consumers to address State and business level protections, and considering privacy and security policies and implementation at a nationwide level.

Ultimately, the effective coordination of health IT activities will help create an environment that improves the health status of both individuals and communities at the same time that personal health information is protected.

The HHS Office of the National Coordinator for Health IT, ONC, is charged with leading the national health IT agenda across the Federal Government and the private sector by coordinating health IT activities, including those related to privacy and security. ONC has the lead for working with CMS, the Office for Civil Rights, or OCR, and others to develop the privacy policies for health IT, and OCR and CMS are responsible for the oversight and enforcement of the related HIPAA rules.

The GAO report provides an excellent summary of the myriad of our successful health IT activities since 2004, and the report documents an active, progressive program of HHS activities that identify national privacy issues to be addressed as well as barriers to interoperability caused by privacy policy variations across States that need to be resolved.

The tools we use to advance our privacy and security activities include contracts, including a recent one with the National Governors Association, an interdepartmental Federal Policy Council, and a public-private Confidentiality, Privacy, and Security Work Group of the American Health Information Community. The Community is a Federal advisory committee that is chaired by Secretary Leavitt himself and plays a central role in all of our activities. The members of the Community, consisting of senior leaders from the public and private sectors, participate in deliberations that guide our work and shape our understanding of how we can most effectively advance the health IT agenda nationwide, including privacy and security.

Much like the historic journey by Lewis and Clark 200 years ago, who were crossing uncharted territory, we, too, are on a similar journey. Their goal was clear: to find a route to the Pacific Ocean, although the exact path was unknown at the beginning. Our goal is clear as well: The secure exchange of interoperable electronic health information. And the detailed milestones necessary to achieve our goal are also not yet knowable.

Our approach is iterative. First, it requires an understanding of the multiple environments in which we are operating. To gain this understanding, we have initiated multiple complementary activi-

ties, such as the Nationwide Health Information Network prototypes, the Privacy and Security Solutions Contract, and the State Alliance for e-Health. And we have gathered input from other expert resources such as the National Committee for Vital and Health Statistics, or NCVHS.

Second, our approach requires that we evaluate and analyze what we have discovered and learned. For example, only after we get the State level reports this spring that identify challenges and opportunities to protect and share health information will we have sufficient data to reliably establish the next set of milestones that we must achieve. An output from one source becomes input for another, such as the NCVHS recommendations that have been publicly shared with the Community work group I mentioned previously. As that work group moves from addressing security to addressing privacy concerns, we anticipate that these recommendations will inform the next set of privacy priorities.

Our activities confirm the importance we give to confidentiality, privacy, and security. We have been executing an effective plan, originally described in our strategic framework that you mentioned, Mr. Chairman, and one that will continue to grow and evolve as we submit our health IT strategic plan later this year.

We are using a results-oriented strategy of discovery and advancement that must be done in collaboration with a variety of stakeholders at the local, State, and national levels. GAO has documented the progress that we have made in the first 2 years of our work, and we continue to undertake multiple related productive activities to properly protect the electronic health information today, tomorrow, and into the future.

Thank you for your time, and I welcome any questions you might have.

Chairman AKAKA. Thank you very much. I want our witnesses to know that your full statements will be included in the record.

Mr. Green.

TESTIMONY OF DANIEL A. GREEN,[1] DEPUTY ASSOCIATE DIRECTOR, CENTER FOR EMPLOYEE AND FAMILY SUPPORT POLICY, OFFICE OF PERSONNEL MANAGEMENT

Mr. GREEN. Mr. Chairman, Members of the Subcommittee, it is my pleasure to be here today to represent the Office of Personnel Management (OPM) Director Linda Springer. I plan to discuss how OPM is working with the Department of Health and Human Services and other organizations on the National Health Information Technology Initiative, and I will discuss how we at OPM are working with our health benefits carriers to implement health information technology (IT) that is secure and protects member privacy.

OPM administers the Federal Employees Health Benefits (FEHB) Program, which covers approximately 8 million Federal employees, retirees, and their dependents. Like other large employers, we contract with private sector health plans. We have consistently encouraged participating plans to be responsive to consumer interests by emphasizing flexibility and consumer choice. We have also encouraged plans to adopt health information technology as an

[1] The prepared statement of Mr. Green appears in the Appendix on page 44.

important consumer-oriented initiative. At the same time, we have placed great importance on the privacy and security of personal health information.

FEHB enrollees have the same privacy protections under Federal law as all Americans. The Health Insurance Portability and Accountability Act of 1996, provides protections for privacy of individually identifiable health information. All FEHB health carriers are required to comply with HIPAA requirements.

And now I would like to provide some background on OPM's initiatives in health information technology.

In 2004, President Bush issued an Executive Order to develop and implement a nationwide health IT infrastructure to improve the quality and efficiency of health care. In response to the Executive Order, we have been working with our FEHB plans on focused efforts to promote health IT while at the same time ensuring compliance with Federal requirements on privacy and security. More specifically, we have asked our carriers to concentrate on specific short-term objectives which include education for consumers on health IT, offering personal health records to consumers based on their medical claims history, encouraging e-prescribing, linking disease management programs with health IT, and compliance with Federal requirements on privacy.

We have found that while there are wide variations in the scope and extent of health IT use, most carriers have focused on providing consumers with claims-based information through their secured websites. Some have robust health IT systems. We have recognized them on our own website during Open Season so consumers would have this additional information to take into consideration in making their plan choices.

Then, last August, President Bush issued a second Executive Order, which underscored his commitment not only to health IT, but also to health care cost and quality transparency. In support of the order, we required all FEHB carriers to report on quality measures, including data from the Health Plan Employer Data and Information set. We also encouraged them to provide information on cost and quality transparency. Along with the carriers that have state-of-the-art health IT capabilities, the carriers that made their best efforts to provide cost and quality transparency were also prominently positioned on our Open Season website last fall.

Looking forward, OPM will continue to work with carriers on standards for interoperability of health information records as they are adopted in the health care industry, and we will continue to provide information for consumers on carriers' cost and quality transparency initiatives as well as their health IT capabilities.

As a member of the American Health Information Community, OPM will monitor the recommendations of the Confidentiality, Privacy, and Security Work Group and determine if there are privacy and security requirements that should be applied to FEHB carriers. We firmly believe privacy and security of personal health information is important. We are encouraged by HHS's efforts to address this important issue. We plan to continue to work closely with HHS, the Community, and the Health IT Policy Council to ensure all necessary steps are taken to protect consumer privacy rights.

We appreciate this opportunity to testify before the Subcommittee on this very important issue, and we will be glad to answer any questions you may have.

Chairman AKAKA. Thank you very much for your testimony.

Dr. Kolodner, the GAO report notes that HHS disagreed with GAO's recommendation to define and implement the overall approach for protecting health information, including identifying milestones and integrating privacy efforts. Can you elaborate on HHS's objection to GAO's recommendation, particularly why HHS believes that setting milestones will impede progress and preclude stakeholder dialogue?

Dr. KOLODNER. Yes, Mr. Chairman. As I mentioned, the issue is not whether we have milestones. Milestones that we can set up right now based on what we know are very high level. They are, for example, to complete our Privacy and Security Solutions contract, to get the results of the contract, to analyze those results, and based on the content that was given in those analyses, to then determine the next set of milestones. That is pretty high level. That is not what we believe GAO was telling us to do, because that is basic project management, and we are doing that already.

The idea of stating right now what those milestones will look like in June or July, when we have not yet received the report that will be received this spring, is something that we know would probably not accurately reflect what we will be executing in June, July, and August. So we see this as an iterative process of discovery and collaboration.

A very important reality is that there are many parties that have very strong feelings, as you can tell, about this area, and privacy is important. We need to make sure that we advance deliberately, advance as quickly as we possibly can, but to make sure that we listen to and are informed by a variety of viewpoints. And as those deliberations occur and as those collaborations occur, we will advance forward.

Chairman AKAKA. Thank you.

Mr. Green, OPM's contracts with carriers require compliance with HIPAA. As part of OPM's requirement to promote the use of health IT, the 2007 Call Letter required carriers to comply with Federal requirements to protect the privacy of individually identifiable health information.

How does OPM monitor carriers' compliance with HIPAA privacy and security rules? And what steps are taken if a carrier is found to be noncompliant?

Mr. GREEN. Mr. Chairman, in addition to the HIPAA law, we have required by contract that all our carriers follow the HIPAA rules, and we have also added privacy requirements that pre-date the HIPAA law, and those are in our standard contracts. We have also added certain measures that all our carriers are required to comply with concerning confidentiality of records and privacy and the regulations used to supplement the Federal Acquisition Regulations. They are called FEHBAR. The FEHB Acquisition Regulations apply to all our carriers. They are required to notify their contracting officer whenever they have an enforcement action resulting from noncompliance, as issued by a State or Federal authority. They are also subject to audit by both GAO and OPM, including

OPM's Inspector General's office, and they run a system of audits against the computer systems of all our carriers on a rotational basis. And they will be introducing additional privacy audit steps this year into that audit.

Chairman AKAKA. Mr. Green, are there any circumstances that would result in electronic health records or personal health record networks being developed or used by FEHBP carriers that would not come under HIPAA?

Mr. GREEN. Senator, the FEHB carriers are required to follow HIPAA rules, and so are their business associates, such as pharmacy benefit managers. So any subcontracts they have would also under our contract require them to follow HIPAA rules.

Chairman AKAKA. Dr. Kolodner, the statutory advisory committee, NCVHS, and the Secretary's advisory committee, AHIC, have made recommendations to the Secretary of HHS regarding the protection of personal health information. What is HHS's response to the recommendations, and how will they be incorporated into a nationwide health information architecture?

Dr. KOLODNER. Mr. Chairman, the NCVHS recommendations, which were accepted by the Secretary and then sent to the AHIC work group—the Confidentiality, Privacy, and Security Work Group—are, in fact, informing that group as they consider the various privacy policies and privacy priorities. Those will then come back to the Community for recommendation up in terms of specifically what kinds of privacy policies and security kinds of architecture should be required as we move forward.

The Nationwide Health Information Network prototypes also have brought forth a number of different solutions, and we have been using those to look at what should go forward for the next round of trial implementations that we plan to fund this next year. So they are very much guiding and identifying those requirements that need to be moving forward.

Chairman AKAKA. Mr. Green, I believe privacy protections must be built into the health IT architecture at the beginning instead of racing to address privacy violations after Americans lose trust in the system. However, after reading the testimony of the witnesses on our second panel, I fear that HHS is not acting fast enough to integrate privacy protections in the development of the health IT.

With this in mind, Mr. Green, what risks are there to Federal employees' health information as FEHBP carriers push forward with health IT initiatives?

Mr. GREEN. Senator Akaka, nothing in this world is perfect, and there is no absolute certainty anywhere. However, I am convinced that with the procedures that we have in place, the requirements we have in place today, protect our FEHB enrollees as fully or more so than any other citizen in this country against a chance of inappropriate misuse of that information.

In addition, going forward with the implementation of health information technology, we are pleased and honored and excited about our participation in much of the work with the Department of Health and Human Services. As you know, we are a member of the AHIC. We are on several of the subcommittees, working groups, and, in fact, Director Springer for a time chaired the Consumer Empowerment Work Group, which is our deep interest be-

cause we feel like that is our responsibility—to support and protect our enrollees. They are our primary customers, after all. And, in addition, we work with the other Federal agencies that are heavily involved in this as part of an HIT Policy Council.

So I am convinced that as we go forward, our Federal employees, retirees, and survivors and their family members will be as protected as we can possibly make them, and that is our promise to you, sir.

Chairman AKAKA. Thank you. Senator Voinovich.

Senator VOINOVICH. Thank you.

Dr. Kolodner, do you believe that the Office of National Coordinator has sufficient authority to facilitate communications among Federal entities, the private sector, and consumer organizations to lead the development and implementation of appropriate privacy standards?

Dr. KOLODNER. Yes, sir, I believe that we do, and I think that we have a number of avenues and a number of venues where we are already doing that, including the American Health Information Community, and also a number of the contracts with the States, like the State Alliance for e-Health.

Senator VOINOVICH. Do you think outside groups looking in would say that they agree with you?

Dr. KOLODNER. We have several venues where we use public-private collaborations, and we certainly look for any other opportunities there might be, but we have been as open as possible in the development of the standards, and in deliberations by any of the work groups. They are all open, broadcast on the Web, and have opportunities for public comment throughout.

Senator VOINOVICH. I know this is off the subject, but it is something I am interested in. We have not passed appropriations, and we are talking about a continuing resolution. I would be interested in your observations in regard to whether you feel that it has been harmful to your respective organizations to have a continuing resolution in which you are operating under.

Dr. KOLODNER. For the Office of the National Coordinator, we have been able to proceed on a variety of activities that we have underway, and we have not had to slow down because of the continuing resolution. And we also, as you know, have the good fortune of having both Secretary Leavitt's very strong backing—this is one of his top programs—as well as the President having passed two Executive Orders that allow us to move forward.

Senator VOINOVICH. So no problem?

Dr. KOLODNER. No problem.

Senator VOINOVICH. Mr. Green.

Mr. GREEN. Senator, I cannot speak for all of the Office of Personnel Management on our budget issues. I will leave that to Director Springer. I can say that we are moving forward on our initiatives, and we have a very large agenda within the Federal Employees Health Benefits Program and the other benefit systems, and we are moving forward without slackening at all.

Senator VOINOVICH. Do you have the personnel and resources to get the job done?

Mr. GREEN. Sir, I argue and fight for as many resources as I can get with my leadership, but I think that would probably be best left inside the OPM doors.

Senator VOINOVICH. Well, one of the things that bothers me is that we are asking many agencies to do all kinds of things, and we do not allocate the resources so they can get the job done. I know it is very difficult for the secretaries of these departments to be forthcoming about it, but it seems to me that during this new budget cycle we ought to be encouraging both of you to make it clear to the folks that are in charge if you need additional help. I just read, Senator Akaka, where the President is talking about flat funding the nondefense discretionary budget again. We just cannot keep going this way. There are too many responsibilities that are not getting done, and the nondefense discretionary budget is being cut. To be candid with you, we should be paying for the war, just not putting it on the tab. What it is doing is it is squeezing out other priorities that are essential.

Have you, Mr. Green, had a chance to look at the bill that I joined Senator Carper in introducing, the Federal Employees Electronic Personnel Health Records Act?

Mr. GREEN. Yes, sir, I have.

Senator VOINOVICH. I would be interested in your comments about it.

Mr. GREEN. Several comments, as a matter of fact.

We note that the bill is consistent with the direction of the health care industry and the leadership provided by HHS, and it is also consistent with OPM's initiatives, as well, to move our carriers toward having PHRs. We do have some concerns about some of the aspects of the bill. Let me put it this way: We would be excited and would like to work with you and your staff and Senator Carper to move that forward, to deal with some of the issues we have. I think you will find them good points that we both want to work through, and we would be happy to do that with you, sir. But overall, yes, we do support a bill like that.

Senator VOINOVICH. So if Senator Carper's and my staff got in touch with you, you would be able to tell us your concerns.

Mr. GREEN. We would be pleased to do that. Yes, sir.

Senator VOINOVICH. I was glad to hear from your testimony that you are interested in HIT yourself. I mean, it is not like we are asking you to do something that is not already being done.

Mr. GREEN. No, that is true. And our carriers are interested as well. They see this as a real opportunity not only to provide for their members, but also to differentiate themselves in the marketplace. Our job and Mr. Kolodner job is to see to it that they are done interoperably and so that it is portable and also so that they are, in fact, secure, private, and the information is confidential and under the control of the enrollee.

Senator VOINOVICH. Our thought is that we could use that as kind of a model for the rest of the country. I mentioned that I spoke with Aetna, while at the bipartisan health policy conference sponsored by the Commonwealth Fund and the Alliance for Health records with Aetna's CEO, who said he thinks implementing personal health records is a great first step, and that they seem to be

interested in moving forward with it. So it would be wonderful if we could get the standards in place and get moving.

Mr. GREEN. Aetna is one of our carriers, of course, a very large participant, so that is good to hear.

Senator VOINOVICH. Thank you, Senator Akaka.

Chairman AKAKA. Thank you, Senator Voinovich.

Dr. Kolodner, you testified that the current HIPAA statute provides the flexibility to protect health information while allowing best practices to emerge. However, as Mr. Rothstein on our next panel notes in his written testimony, some private sector companies are using electronic health record and personal health record networks that generally are not subject to any Federal or State regulation because the initiatives are not covered entities under HIPAA.

Does HHS have a list of entities that may have access to personal health information under a health IT network, but are not covered by HIPAA?

Dr. KOLODNER. The HIPAA rules define the entities that are covered by HIPAA. There are other entities that are not covered by HIPAA, and he may be referring to some of those entities.

The Confidentiality, Privacy, and Security Work Group and our Consumer Empowerment Work Group, which is another work group under the American Health Information Community, both have started to consider whether there are entities that should be covered under HIPAA that are not now being covered. We will be looking at those recommendations as they come forward and see whether there is sufficient authority in HIPAA to extend that. So we are considering that as part of the deliberations that I mentioned that are underway.

Chairman AKAKA. Dr. Kolodner, HHS has been without a permanent National Coordinator for Health IT since May 19, 2006. When will a permanent National Coordinator be named?

Dr. KOLODNER. Mr. Chairman, that would be a question that Secretary Leavitt would ultimately need to answer. He has asked VA to detail me over. VA did that starting in September. VA was gracious enough to extend the detail, so I will be here for another period of time, and it will be up to Secretary Leavitt to ultimately decide.

Chairman AKAKA. Thank you.

Mr. Green, you testified that OPM is a member of several work groups focused on health IT. Can you share with us some of the recommendations that OPM has made to these groups?

Mr. GREEN. Senator, the work groups operate under a consensus-based decisionmaking process. We contribute to those discussions on each recommendation as they come up.

One of our primary objectives is to ensure consumer rights and responsibilities are protected, and we also share our knowledge on employer-based health benefits to shape recommendations that are achievable and promote the broad goals of the HIT initiative.

Chairman AKAKA. Thank you. Senator Carper.

Senator CARPER. Thanks, Mr. Chairman. Who did you succeed in your job?

Dr. KOLODNER. Dr. David Brailer was the first National Coordinator.

Senator CARPER. What is Dr. Brailer doing now?

Dr. KOLODNER. I believe he is doing some private consulting. He is also a Special Government Employee, since he does still co-chair the American Health Information Community.

Senator CARPER. Thanks. If you ever see him, give him my best. Thanks. All right.

Dr. KOLODNER. I will do so.

Senator CARPER. I understand when I was out of the room in another meeting here in the anteroom that Senator Voinovich asked for some reaction from both of you to the legislation we are about to reintroduce. And I understand that you pretty well trashed it. [Laughter.]

No. I understand you were pretty generous. Would you just recap for me what you had to say and any thoughts you might have for making it better?

Mr. GREEN. Certainly, Senator. I explained that we have reviewed and commented earlier, at least within the Executive Branch, on the bill and that since the provisions in the bill are consistent with the direction that the health care industry is going and the leadership that HHS is providing, it is also consistent with OPM's direction of where we want to move with our carriers in the FEHB program. So we are supportive of the bill and its outline and its purpose. There are some issues that we would like to have the opportunity to discuss with you and your staff that we think we can help improve the bill to fit what goes on within the FEHB program and some other issues, to help deal with privacy concerns as well. So we would welcome the opportunity.

Senator CARPER. We gratefully accept that offer.

I mentioned earlier in opening statement, that in Delaware we are standing up the Delaware Health Information Network, and we are doing so with the financial support from the Department that Secretary Leavitt leads and from some of the folks that are your colleagues, Dr. Kolodner. And the State of Delaware is matching that money over the next couple of years, and the private sector in our State is stepping up as well. We just learned that Blue Cross/Blue Shield of Delaware is the latest to step forward and say they want to be financially supportive of this, too. So we are very much encouraged.

One of our focuses in standing up the Delaware Health Information Network is to protect patient privacy and patient records. And I know that you come out of the VA, don't you?

Dr. KOLODNER. Yes, sir.

Senator CARPER. How long did you work there?

Dr. KOLODNER. Twenty-eight years.

Senator CARPER. Twenty-eight years, wow. Did you start as a child? [Laughter.]

But the VA approach on harnessing information technology—just talk with us a little bit about what you did there to protect the privacy of patients and their personal or health records. And is there maybe a lesson there, a model for the rest of us, whether we are doing it at the State level or for Federal employees?

Dr. KOLODNER. The VA had privacy as a central part of the system from early on, and we actually—because it is a single system and not a network. A network obviously presents new opportuni-

ties, new challenges. But as a system, we actually would contract to security companies for them to try to break into the electronic health record system and find where the vulnerabilities were so that we could fix them before any breach had occurred. The VistA system, which started out as the Decentralized Hospital Computer Program is secure and has not been a source of any breaches.

We also have a personal health record we provide to veterans, starting in December, we actually upload this robust data from.

Senator CARPER. Starting this past December?

Dr. KOLODNER. This past December. We had it in test with a few thousand veterans before that, but starting this past December, veterans can, in fact, have a copy of their clinical record—not just any claims data but the clinical data that is in this robust VistA system—uploaded to a personal health record if they choose. So it is an opt-in strategy. And we have security——

Senator CARPER. It is opt in, not opt out?

Dr. KOLODNER. It is opt in for the personal health record, yes, sir. And we have gotten very positive response from the veterans who——

Senator CARPER. Are they opting in?

Dr. KOLODNER. They are opting in. Hundreds of thousands have opted in so far. And as with any new technology, if you remember when the Internet started, many of us were a little skeptical. We wanted to see what was going on. Did we want to use our credit card over the Internet? And gradually what happens is you get the early adopters who were willing to take a chance, and the system gets more and more robust, more and more trusted, and more people, in fact, come on board. So there is a growth curve that is a natural growth curve. It is not that everybody comes on at once. But it is one where you get more rapid uptake over time, and we are beginning to see that, particularly as you offer services that—veterans had wanted to be able to refill their prescriptions online, and they can do that now.

Senator CARPER. Great. You may recall in the last Congress the Senate passed legislation dealing with health IT, passed a pretty good bill. I don't know that there was anybody who voted against it in the Senate. It went over to the House and it died. It died over there, and for reasons that are not altogether clear to me.

What advice would you have for us as we come back and take up the legislation? There may be an effort to try to combine what Senator Voinovich and I are doing to actually make it part of the larger piece of legislation? I don't know if we will let that happen. Maybe we will, maybe we won't. There could be worse outcomes.

But why did it die in the House? What might be different this time? And as we tinker with that legislation and prepare to pass it again in the Senate, what advice would you have for us, either of you?

Dr. KOLODNER. Senator, certainly the reason why it died in the House or why the Senate and the House could not get together on it is beyond my purview and my expertise, and I would leave that to you and your colleagues.

Senator CARPER. Well, we do not know either. [Laughter.]

But we will figure it out.

Dr. KOLODNER. I know that there is great interest in the health IT bill, and certainly we will work with you and with your colleagues as the various bills go forward to certainly work on something that advances the whole health IT agenda.

Senator CARPER. Well, I don't know how familiar you were with the legislation that was enacted in the Senate. I am not going to dwell on it. But if you have any ideas for the record that you might like to suggest to us, either of you, for how to improve that legislation when it comes to the floor, which I think will come fairly soon, we would welcome your input.

Do you all have anything else you want to say with respect to any of the questions I have raised here?

[No response.]

OK. Thank you. Thanks very much for your good work, particularly at the VA, and as a veteran myself of the Navy, you make us very proud, even prouder to be veterans. And for all the veterans around the country, in Delaware and other places, who have the opportunity to use what I call the gold standard for health care in this country today, thank you for helping to provide that system.

Chairman AKAKA. Senator Voinovich.

Senator VOINOVICH. I would like to get back to the bill that Senator Carper and I are going to reintroduce. It is my understanding that originally the bill had a 1-year requirement, the bill Senator Carper had, and then we had a 2-year requirement, and then we talked to OPM and they said we might be moving too quickly.

It is my understanding that OPM is reluctant to agree to a statutory deadline because the HHS standards have not been published. However, Dr. Kolodner, you indicated that you have the team necessary to get the job done. I just want you to know I do not want to see publication of the standards delayed. If you do not have the people that you need to get the job done, then we ought to know about it. I will pick up the phone and call my good friend, former Governor Mike Leavitt, and say, "Mike, you guys have made a commitment. Now put the resources in it so we can get it done." I want this taken care of.

So if you want to respond to that, you may. [Laughter.]

Dr. KOLODNER. One of the pleasures of being over at HHS has been the undying support of Secretary Leavitt for the area of health IT. I could not ask for any stronger support from him, and that has been one of the things that attracted me to take this interim appointment.

The office actually was established a little over a year ago, and we are just finishing up staffing up to our authorized level. We had been filling those activities with contractors. We are now bringing on the staff that we need, and we are moving as fast as we believe that we can, again, with this iterative process that is necessary to make the best policy.

Senator VOINOVICH. Well, we welcome your input on our legislation. We will be talking to you and Mr. Green about it more.

Thank you, Senator Akaka.

Chairman AKAKA. Dr. Kolodner and Mr. Green, thank you very much for your valuable testimony. I look forward to working with each of you to ensure that privacy and security are integral parts of the health IT architecture. Thank you very much.

Dr. KOLODNER. Thank you, sir.

Mr. GREEN. Thank you.

Chairman AKAKA. And now I ask our second panel of witnesses to come forward. Testifying on our second panel are David Powner, Director of IT Management Issues, and Linda Koontz, Director of Information Management Issues, from the Government Accountability Office; also Mark Rothstein, Director of the Institute for Bioethics, Health Policy, and Law at the University of Louisville School of Medicine, as well as the Chair of the Subcommittee on Privacy and Confidentiality of the National Committee on Vital and Health Statistics; and Dr. Carol Diamond, Managing Director of the Markle Foundation.

As you know, it is the custom of the Subcommittee to swear in all witnesses, so please stand and raise your right hand. Do you swear that the testimony you are about to give before this Subcommittee is the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. POWNER. I do.

Ms. KOONTZ. I do.

Mr. ROTHSTEIN. I do.

Dr. DIAMOND. I do.

Chairman AKAKA. Thank you. Mr. Powner, please proceed with your statement.

TESTIMONY OF DAVID A. POWNER,[1] DIRECTOR OF INFORMATION TECHNOLOGY MANAGEMENT ISSUES, ACCOMPANIED BY LINDA KOONTZ, DIRECTOR OF INFORMATION MANAGEMENT ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. POWNER. Chairman Akaka, Ranking Member Voinovich, we appreciate the opportunity to testify on privacy initiatives associated with our Nation's efforts to increase the use of health information technology. With me today is Linda Koontz, GAO's Director of Information Management Issues and privacy expert.

In 2004, President Bush issued an Executive Order that called for widespread adoption of electronic health records by 2014 and established a National Coordinator for Health IT to lead and to foster public-private coordination. Over the past several years, we have issued several reports and testified on numerous occasions, highlighting the need for detailed plans, milestones, and mechanisms to monitor progress if this 10-year goal is to be achieved.

The benefits of health IT are immense and include reducing medical errors. However, it also raises concerns regarding the extent to which patient privacy is protected. The challenge here is to strike the right balance between patient privacy concerns and the numerous benefits IT has to offer this industry.

This afternoon, as requested, I will summarize our report completed at your request, Mr. Chairman, on HHS's health IT privacy initiatives. Specifically, I would like to highlight three points: First, the importance of having a comprehensive privacy approach; second, HHS's initial efforts to address privacy; and, third, additional actions needed.

[1] The prepared statement of Mr. Powner and Ms. Koontz with attachments appears in the Appendix on page 52.

Privacy is a major concern in the health care industry given the sensitivity of certain medical information and the complexity of the health care delivery system with its numerous players and extensive information exchange requirements. This concern increases as our Nation transitions to using more electronic health records. A comprehensive privacy approach is needed so that ultimately it is clear who these records are disclosed to, what limitations are placed on the use of the information, how patients can access their records, how inaccurate or incomplete information is corrected, and what administrative, physical, and technical safeguards are needed to protect electronic health information.

HHS acknowledges in its National Health IT Framework the need to protect consumer privacy and plans to develop and implement appropriate privacy and security policies, practices, and standards for electronic health information exchange. HHS and its Office of the National Coordinator have initiated several efforts to address privacy. These include: Awarding several contracts that includes one for privacy and security solutions; consulting with the National Committee on Vital and Health Statistics to develop privacy recommendations; and forming a Confidentiality, Privacy, and Security Work Group to identify and address privacy and security policy issues.

These efforts are good building blocks, but much work remains, including: Assessing how variations in State laws affect health information exchange; reporting and acting on the privacy and security contractors' findings; acting on advisory group recommendations; and identifying and implementing privacy and security standards.

The National Coordinator's Office intends to use the results of these activities to identify policy and technical solutions for protecting personal health information as part of its continuing effort to complete a national health IT strategy. Ultimately, these and other efforts are to result in a comprehensive security and privacy policies, practices, and standards. However, how HHS plans to integrate the outcomes of its initiatives and when is unclear.

Therefore, we recommended, Mr. Chairman, that HHS develop an overall privacy approach or a game plan that identifies milestones and an accountable entity for integrating the outcomes of its health IT contracts and recommendations from advisory groups. In addition, this approach should ensure that key privacy principles highlighted in our written statement are fully addressed. And, finally, this approach should address key challenges associated with legal and policy issues, disclosure of information, individual rights to access, and security measures.

In summary, Mr. Chairman, while progress continues to be made through the National Coordinator's private initiatives, a comprehensive approach is needed to integrate the results of the initiatives to ensure that key privacy principles are addressed and to ensure that recommendations from the advisory committees are effectively implemented. Otherwise, HHS will not be providing the leadership called for by the President and its goal of safeguarding personal health information will be in jeopardy.

This concludes our statement. We would be pleased to answer questions.

Chairman AKAKA. Thank you very much, Mr. Powner. Mr. Rothstein.

TESTIMONY OF MARK A. ROTHSTEIN,[1] HERBERT F. BOEHL CHAIR OF LAW AND MEDICINE, AND DIRECTOR, INSTITUTE FOR BIOETHICS, HEALTH POLICY AND LAW, UNIVERSITY OF LOUISVILLE SCHOOL OF MEDICINE

Mr. ROTHSTEIN. Yes, thank you very much, Mr. Chairman and Senator Voinovich. I appreciate the opportunity to be with you this afternoon. I want to clarify for the record that I am appearing in my individual capacity and not as a representative of NCVHS, which may want to deny any responsibility for my statements, written or oral.

I want to make two points this afternoon. First, in my view, HHS has not made meaningful progress in developing and implementing measures to protect the privacy of health information in electronic health networks. And the second point is that time is of the essence. I believe HHS must begin to act immediately on these very difficult privacy issues and also that Congress needs to hold HHS accountable and make them meet the milestones that have been suggested by GAO or some of the other measures that I want to suggest to you this afternoon in my testimony.

I specifically agree with the comments in the GAO report. I believe that they accurately captured the sense and the progress, or lack of progress, on the privacy issues. But I would add my own assessment that I believe that the focus on privacy is currently lagging behind the focus at HHS on technical development of the infrastructure of the NHIN. And I am concerned that the gap between the technical progress and privacy is actually widening, and that is not a luxury that we have, for reasons that I want to pursue in just a minute.

In 2004, the head of ONC at that time, Dr. Brailer, asked NCVHS to do a comprehensive study on privacy and confidentiality issues in the Nationwide Health Information Network. And it took us 18 months of hearings throughout the country, dozens of witnesses, and lots of rather heated deliberation to reach our recommendations, which were delivered to the Secretary in June 2006. And just to emphasize the nature of these fundamental questions that have to be resolved, I want to go through a couple of them with you, if I may.

First, NCVHS noted that a decision has to be made on whether individuals have a right to decide whether they want to be a part of this nationwide system, and if so, should that be opt in or opt out or some combination, should it be controlled locally or via some other method. So that is a fundamental question.

Another fundamental question is whether individuals should have some control over the contents of their health records that would be disclosed via the NHIN. When you put together comprehensive, longitudinal, individual health records, they are likely to contain lots of old data. Some of it may be very sensitive. Some of it may be irrelevant to current care. These records are not usually available now because of the fragmentation of the system. You

[1] The prepared statement of Mr. Rothstein appears in the Appendix on page 130.

cannot get it from all these places. Electronically, it will be easy to obtain this information, and I am concerned that under an electronic system we should not have less privacy than we do today. So that is a concern of mine.

I am also concerned about the scope of the disclosures when people have to sign an authorization to get a job or life insurance. About 25 million of these are signed each year in the United States, and when the records are released, typically the entire file is sent. And this may include all this sensitive information.

NCVHS submitted 26 recommendations to the Secretary, and I don't think that very much progress, if any, has been made on any of these areas that we identified. And I believe that time is of the essence, as I emphasized in my written testimony. Private sector groups are working today—while we are still talking about these issues officially in terms of regulation, the private sector is marching ahead. Last month, we heard at our hearings from Wal-Mart about this huge personal health record system that it is putting together, with over 2.5 million employees represented, and this is a single company, in collaboration with other employers. They are not health plans. They are not covered entities under HIPAA. There is no regulation in place.

So not only do I support the GAO recommendations, I think we need to be thinking beyond HIPAA. HIPAA is an archaic statute that was designed for totally different purposes. It was designed for the payment system. We now have a more comprehensive nationwide network involved, and I think we have to be thinking more comprehensively. And I believe that there are lots of things that need to be done, and I would recommend that the Subcommittee work with HHS and try to move the ball forward more rapidly on these very important issues.

So I thank you for the opportunity to testify today and I look forward to your questions.

Chairman AKAKA. Thank you very much. Dr. Diamond.

TESTIMONY OF CAROL C. DIAMOND, M.D.,[1] MANAGING DIRECTOR, MARKLE FOUNDATION, AND CHAIR, CONNECTING FOR HEALTH

Dr. DIAMOND. Thank you, Chairman Akaka, Senator Voinovich. It is a privilege to be invited to testify today. I am the Managing Director at the Markle Foundation, and in that capacity I also serve as Chair of a large public-private collaborative called Connecting for Health. Our goal at Connecting for Health is to make sure that vital information is available both for patients and their providers when it is needed and where it is needed in a way that protects privacy and earns the trust of the American people.

As you heard today, numerous efforts are underway to promote the use of health information technology within HHS, other parts of government, and the private sector. Yet as the GAO report and Mr. Rothstein have stated, there has not yet been enough progress in establishing a policy framework that will earn the long-term public trust required to sustain and build upon current activities.

[1] The prepared statement of Dr. Diamond appears in the Appendix on page 138.

Toward that end, I have two important recommendations to make. First, the Nation needs a well-defined, comprehensive privacy framework based on key policy and technology attributes that I will lay out. Second, while the entities and contracts created by HHS have been useful to initiate action in this field, we now need to find the appropriate longer-term process for determining both the policies and the technologies that will achieve the attributes of such a framework. Our national strategy for health information technology must be carried out by decisionmakers informed by and accountable to a broad range of interests with direct public accountability.

Let me first talk about the required framework for health IT. Our group took 3 years to develop this framework, and the framework includes the attributes that are necessary to protect privacy and security. Efforts to gather and share information should achieve these attributes:

First, information sharing at the national level should be done in a decentralized and distributed way. Simply put, health information sharing should not require the development of large centralized repositories of personal health information. Clinical data should be left in the hands of patients and those who have a direct relationship with them in their care, and leave decisions about who should or should not see that data with patients and providers directly involved with their care.

Second, sharing should separate demographic and clinical information. Sharing should be accomplished with an index that does not contain clinical data but, rather, knows where relevant information resides. Only those with proper authorization are then allowed to access the information, and this does not require the use of a national identifier.

Third, the framework should be a flexible platform for innovation. Participation in the network by a broad range of providers delivering products and services will be a result of using open standards and transparent policies. This will encourage innovation so that we can make critical rapid progress.

Fourth, the framework should implement privacy through technology. This is a key attribute. Technology choices should be made so that they can enable the effective implementation of policies protecting privacy. These technologies should create audit trails, implement security, improve data accuracy, prevent both intentional and unintentional improper disclosure of information. They should build rules and permissions into the process of accessing and distributing data.

Our fifth attribute is really a set of nine foundational privacy principles. These have been adopted from fair information practices and other sources internationally. These principles include things like transparency, specifying the purpose of data being collected, collecting only what is necessary, adhering to the uses agreed to by the individual, allowing the individuals to know and have a say in how their information is used, maintaining the integrity of data, audit, oversight, and remedies in the event of breach or misuse. Every health information initiative should be expected to disclose how it addresses each of these principles.

In summary, HHS deserves praise for its success in elevating public and industry interest in health information exchange and for encouraging the adoption of technical standards. But focusing only on technical standards is like building an interstate highway system, without the rules for entering, exiting, or anticipating the speed limits that need to be accommodated. In order to serve the communities through which it passes, a highway must have a coherent set of rules, made obvious through signage and visibly enforced, and be embedded in the design of the highway itself. And for the users of health information, patients and their providers, an explicit policy framework is essential.

Several years of public opinion surveys show that Americans have significant privacy concerns when it comes to their health information. Without a policy framework with the attributes we propose, our Nation runs the risk of inappropriate uses of personal information followed by public clamor for hasty remedies, which will undermine the sustainability of an information sharing network. And these policies that touch the most private concerns of every American require a clear framework for privacy and an accountable visible process that can encourage public interest, that will be maintained over time, and that will give consumers confidence that their interests are being looked after.

Mr. Chairman, the lack of trust in health information technology may not only impede progress but, more profoundly, it may squander this amazing window we have to stimulate a much needed transformation of our overburdened health care system.

Thank you for the opportunity to testify.

Chairman AKAKA. Thank you very much for your statements.

I just talked to my friend, Senator Voinovich, and I am going to let him proceed first.

Senator VOINOVICH. Thank you very much, Senator Akaka.

First of all, you heard the testimony of Dr. Kolodner. You were here for his testimony, and I asked him whether or not he had the staff to get the job done. In your opinion, does he have the staff to get the job done?

Mr. POWNER. We specifically have not looked at whether he has the human capital and all the resources to get the job done. Our big concern, Ranking Member Voinovich, is that we do not see a road map to get from where we are at today to have a comprehensive privacy policy in place.

Dr. Kolodner made some comments about sound project management. Sound project management is about having milestones and targets, and we go after those milestones and set interim performance measures to gauge whether we are making enough progress or not. That is what we do not see, sir.

Senator VOINOVICH. OK. So you are saying plan, milestones and, in addition, metrics to judge if milestones are being met?

Mr. POWNER. Absolutely, and some of our other witnesses mentioned some of the key privacy principles that clearly need to be addressed as part of that approach.

Senator VOINOVICH. Right. Senator Akaka, it might be good—if you recall, what we have been able to do with the GAO High-Risk agencies. OMB and GAO have sat down together to develop a stra-

tegic plan on addressing these problems. They are making progress. It seems that process may have value here.

The last question is for Mr. Rothstein. You said they are lagging behind the technical structure of developing IT. So what you are seeing is fast development without building privacy in at the beginning?

Mr. ROTHSTEIN. Yes, Senator, and there are significant concerns that, unless privacy is built into the architecture of the system, we will not be able to come back and do it later. And that is why privacy protections have to be in from the start, and the longer it takes us to develop policies on what our privacy and confidentiality and security rules are, the more danger we have that it is going to be too late or it is going to be prohibitively expensive to go back and try to add the privacy protections.

Senator VOINOVICH. Just another comment, Senator Akaka. It is nice that OPM may be saying they cannot do it because they are waiting to incorporate the privacy standards into the system. Thank you very much. I appreciate the chance to ask these questions.

Chairman AKAKA. Thank you very much, Senator Voinovich.

Mr. Powner, you recommended in your testimony that HHS define a comprehensive privacy approach that includes detailed plans and milestones for integrating its various initiatives. GAO specifically mentioned the need to sequence the implementation of key activities appropriately. Would you explain that comment? Tell us why this is important. And what else is missing from HHS's current approach?

Mr. POWNER. Similar to Mr. Rothstein's comment, the sequencing is very important because his comment about building in privacy and security early, we see many examples throughout the Federal Government, Mr. Chairman, where we built in security or privacy after the fact, after systems and networks are built; and, one, it is very difficult to implement and, two, it is much more costly to do it after the fact. So it is very important that we sequence these activities. We are talking about prototypes right now for the National Health Information Network, and to Mr. Rothstein's point, what is happening is the technology is getting ahead of the policy, and we need to make sure that we get the policies in place so that we can actually make those appropriate technology decisions and build it in up front.

Chairman AKAKA. Dr. Diamond, I agree with your statement that public trust cannot be fully accomplished by relying only on existing legal provisions such as HIPAA. However, Mr. Green testified that OPM is pushing health IT through the FEHBP and is only requiring carriers to follow Federal privacy requirements.

Do you believe OPM can earn the trust of Federal employees when carriers are increasingly using health IT?

Dr. DIAMOND. Chairman, I would say two things. I think it is a very good thing for the Federal Government to help its employees find ways to see and access their own health information. But I would say that in the same way that the government can stimulate the use of information technology and stimulate the expectation that people can have their own information, it can also stimulate the adherence to a basic framework of privacy based on the at-

tributes that I articulated today. As long as those both policy and technology things are clear to the user, that there is transparency, that people know how their information is used, then we can earn the trust.

So I would say there is an opportunity to both stimulate people being more engaged in their health care by having personal health records and also to use the role of the Federal Government to make sure the attributes are built into every initiative that is put out there using information technology.

Chairman AKAKA. Mr. Rothstein, the privacy and security requirements of HIPAA and other laws do not cover all entities that exchange electronic personal health information. What can HHS do to ensure that gaps in legal privacy protection of health information are addressed by a privacy framework for the nationwide health information exchange?

Mr. ROTHSTEIN. Mr. Chairman, one of the specific recommendations in my written testimony is that I believe that HHS should undertake a study to determine the number of health care providers that are, in fact, not covered entities under HIPAA at the moment. We have been doing that in my subcommittee—that is, the Subcommittee on Privacy and Confidentiality—and we are frankly astonished at the number of health care providers that are not covered entities.

Unless you are engaged in an electronic billing transaction, you are not a covered entity. So all of the urgent-care, cash-paid doctors, many cosmetic surgeons that are not covered by any insurance plan, all sorts of other health care providers that are not covered—massage therapists, acupuncturists, and so forth—may not be covered entities under HIPAA. We don't know how many there are, and it seems that it is going to be Congress' role to enact new legislation or to amend the HIPAA statute to bring in all these other health care providers. But I think it would be very helpful to the Congress if we had a sense of how many there are that need to be covered.

Chairman AKAKA. Dr. Diamond.

Dr. DIAMOND. Yes, Chairman. As was stated previously by other witnesses, HIPAA was written at a time where we did not contemplate a Nationwide Health Information Network, nor did we contemplate the number of entities and parties today who are part of the use and sharing of health information.

I do think, as I stated in my testimony, the two comprehensive things to do would be to require a policy framework based on key attributes and to establish a public process to build in and make sure that each information technology initiative that is proposed lives up to those attributes.

Chairman AKAKA. Thank you.

Dr. Diamond and Mr. Rothstein, based on the work of HHS to date to promote health IT, are there any legislative changes that we in Congress should consider making to ensure that the privacy of health information is protected?

Mr. ROTHSTEIN. Senator, I believe there are two areas in which congressional action would be indicated. First, is to extend the coverage of health privacy legislation; in other words, to expand the number of covered entities that are currently covered under HIPAA

or under some other replacement law. The second is of a more substantive nature, and that would be to try to limit the amount of information that third parties can require individuals to provide as a condition of getting a job or a life insurance policy or some other commercial transaction. At the moment, it is lawful to require that individuals sign basically an unlimited release and then all this information and, increasingly, more comprehensive information will be disclosed electronically to people who do not have a legitimate interest in this extra information. An employer or insurer may have a legitimate interest in knowing your current health status, but maybe not things that happened 20 or 30 years ago that would be of a very sensitive nature. And I think restricting those kinds of information requests would be very helpful.

An example would be under the Americans with Disabilities Act, the Federal statute dealing with disability discrimination says that if you are a current employee, the employer can only ask about job-related health information. But if you are an individual who has a job offer but have not started yet, then they can have an unlimited request for information. If you applied that same standard that is applicable to current employees to these applicants, then the amount of information would be reduced substantially.

Chairman AKAKA. Dr. Diamond.

Dr. DIAMOND. I think there is an opportunity right now to consider what the right process is for this next level of public input and discussion that is required around privacy and security. And I think what I propose in my written testimony is what I will repeat here. Based on a set of foundational principles, there does need to be a process that will have appropriate public input, notice and comment, and deliberation so that we can move forward in a way that people feel trust in the health information network and the way their information is being shared. And I do think reverting to the policies and the attributes that I laid out today serve as a good yardstick or metric for trying to determine how to move forward.

Chairman AKAKA. Thank you. This question is to all of the panelists. You all heard the testimony of OPM that Federal employees' electronic health information is protected, despite the fact that HHS's efforts on privacy and security are lagging behind. Do you agree with OPM? Mr. Powner.

Mr. POWNER. Sir, I do not believe we are in a position to comment on OPM's efforts in that area. We have not looked at it in any detail at all.

Chairman AKAKA. Thank you. Mr. Rothstein.

Mr. ROTHSTEIN. I would only note that the companies that offer insurance to Federal Government employees are covered entities under HIPAA because they are health plans. Therefore, they are regulated in the way that other covered entities are. But individual employees are not protected in the sense that for all of this information that is suddenly going to be aggregated and available electronically at a single point in time, we do not have new rules that apply to the network. What we are applying to government employees are the old rules under HIPAA.

Chairman AKAKA. Dr. Diamond.

Dr. DIAMOND. Yes, I am not familiar with OPM's efforts. I will just offer that under the existing HIPAA rule, there have been 22,000 complaints to OCR, and very few have actually resulted in penalties. And I think there is an opportunity to look at not only these new attributes that I laid out here and the principles as a way to ask ourselves if we are doing enough, but also to look at appropriate remedies in the event of breaches, because we are in an information world today. This is the Information Age, and I think every one of us, while we enjoy the benefits of it, also have to acknowledge that we need to think about the protections that need to be in place to participate fully.

Chairman AKAKA. Mr. Powner, what do organizations that store and exchange personal information consider when balancing the benefits realized from IT with the risks introduced by storing large amounts of personal data in electronic format?

Ms. KOONTZ. I will answer that, if I may. We found, in terms of the research that we have done on privacy, that best practices organizations do a number of things. First of all, they get continuous and early input from stakeholders, from experts, and from the public in some form. And I emphasize the word "continuously" because as these kinds of initiatives are worked on, they tend to evolve and change, and there needs to be a constant going back to the privacy principles to touch them to make sure that we are consistent with the framework that we have selected.

I think successful organizations also use fair information principles. I agree with many of the other witnesses on the panel today that HHS needs to take a broad look at privacy, and it is useful to look at the fair information practices which are broad, very internationally accepted principles as a way of facilitating discussion on the balance that should be struck between privacy and other interests.

I think best practices organizations assess privacy protections, as many of the other panelists have said, before information technology is acquired or developed. Technology can be an enabler to help build in privacy protections, but once a system is built, it is very difficult and often very expensive to go back and retrofit those kinds of protections.

To the extent that HHS uses these kinds of best practices, I think it increases their chance of success in this.

Chairman AKAKA. Thank you, Ms. Koontz.

Mr. Powner, HHS has been without a permanent National Coordinator for Health IT for almost a year. What effect has the absence of a national coordinator had on HHS's progress toward defining a privacy framework as part of its national strategy for health IT?

Mr. POWNER. First of all, I think we need to give some credit to Dr. Brailer for getting the ball rolling here, and Dr. Kolodner has kept it rolling. But longer term, when you look at whether we need a permanent national health IT coordinator, we believe we do, for a couple of reasons. There are going to be some tough decisions. What we discussed here today, tough privacy decisions from a policy perspective are going to have to be made. Having a permanent leader would be very important for that.

Also, too, because of the collaboration that needs to occur with the private sector, having a permanent leader sends a message that this is a presidential priority. Having an interim leader does not.

Chairman AKAKA. Thank you very much.

Mr. Rothstein and Dr. Diamond, in June 2006, the National Committee on Vital and Health Statistics sent a letter to HHS Secretary Leavitt with 26 recommendations on privacy and confidentiality in the Nationwide Health Information Network. Meanwhile, the Markle Foundation is working with various stakeholders, including government, industry, and health care experts, to address the challenges of creating a Nationwide Health Information Network.

What has been the response from HHS on your initiatives?

Mr. ROTHSTEIN. Mr. Chairman, in terms of the NCVHS, we received in the fall a letter from the Secretary acknowledging receipt of our report, but that has been the extent of our official response from the Department.

Chairman AKAKA. Dr. Diamond.

Dr. DIAMOND. Mr. Chairman, we have been involved in many of the discussions within the work groups of the AHIC and also within the NHIN contract, and I think the groundwork that we did in laying out the framework for sharing information with privacy has been very instrumental in those discussions.

However, we have not yet had the opportunity to see those privacy principles or the comprehensive framework that I discussed today make its way into the current initiatives on the NHIN. And to echo what some of the other witnesses have said, we worry that the technology efforts and the standards efforts are moving too far ahead of some of those privacy principles and privacy requirements that the technology should fulfill, that we should not be trying to correct later on.

We know firsthand from doing our own prototype the year prior in three communities—in Indianapolis, Boston, and Mendocino County, California—that it is possible to connect disparate communities with different technologies using privacy and security. But those decisions about privacy and security changed the way technology was implemented. They drove decisions in the way that technology was implemented that we would like to see inform the process going forward.

Chairman AKAKA. Well, I want to thank you, Mr. Powner, Mr. Rothstein, and Dr. Diamond, for your testimonies and also Ms. Koontz, for your responses as well. And I want you to know that you have provided this Subcommittee with valuable information, and we appreciate all that you have done to ensure that Americans' health information is protected.

Today's hearing underscored the need for HHS to integrate privacy into the nationwide health IT infrastructure. We heard repeatedly that individuals must have trust and confidence in the system to encourage them to share their personal health information. If we want health IT programs to succeed, we must have privacy and security protections in place at the beginning. I look forward to working with HHS, OPM, and the various stakeholder groups to make this happen.

As there is no further business, the hearing record will be open for one week for additional statements or questions from Members of the Subcommittee.

The hearing is now adjourned.

[Whereupon, at 4:17 p.m., the Subcommittee was adjourned.]

APPENDIX

BRIEFING MEMORANDUM

BACKGROUND

Studies published by the Institute of Medicine and others have indicated that fragmented, disorganized, and inaccessible clinical information adversely affects the quality of health care and compromises patient safety. In addition, long-standing problems with medical errors and inefficiencies increase costs for health care delivery in the United States. In 2004 alone, health care spending reaching almost $1.9 trillion, or 16 percent of the gross domestic product.*1*

Health information technology (HIT) — the technology used to collect, store, retrieve, and transfer clinical, administrative, and financial health information electronically — is seen as a promising solution to improve patient safety and reduce inefficiencies. Technology has great potential to improve the quality of care, bolster preparedness of the nation's public health infrastructure, and save money on administrative costs. For example, GAO reported that a single 1,951-bed teaching hospital found $8.6 million in annual savings by replacing paper medical charts with electronic medical records for outpatients. This hospital also reported saving more than $2.8 million annually by replacing its manual process for handling medical records with electronic access to laboratory results and reports.*2* Health care organizations also reported that IT contributed other benefits, such as shorter hospital stays, faster communication of test results, improved management of chronic diseases, and improved accuracy in capturing charges associated with diagnostic and procedure codes.

Studies by the Center for Information Technology Leadership identified savings from the widespread adoption of HIT. *The Value of Healthcare Information Exchange and Interoperability* identified $78 billion in annual savings based on electronically sharing health care data between providers and stakeholders, which resulted in saving time and avoiding duplicate tests. *The Value of Computerized Provider Order Entry in Ambulatory Settings* estimated $44 billion in annual savings based on avoidance of unnecessary outpatient visits and hospital admissions, as well as more cost-effective medication, radiology, and lab ordering. The Center acknowledges that these estimates are based on limited data and a number of assumptions and, therefore, are not necessarily complete and precise. In October 2003, GAO reported significant financial benefits realized from the implementation of health IT, including cost savings at the Department of Veterans Affairs (VA) and expected savings at the Department of Defense (DoD).*3*

Examples of HIT include:

- Electronic health records (EHRs) provide patients and their caregivers the necessary information required for optimal care while reducing costs and administrative overhead, such as that associated with patient registration, admission, discharge, and billing.

---

1 Government Accountability Office "Health Information Technology: HHS is Continuing Efforts to Define a National Strategy," March 15, 2006 (GAO-06-346T).
2 Id.
3 Government Accountability Office, "Information Technology: Benefits Realized for Selected Health Care Functions, October 2003 (GAO-04-224).

- Computer-assisted clinical decision support tools increase the ability of health care providers to take advantage of current medical knowledge from online medical references as they make treatment decisions.
- Computerized provider order entry allows providers to order tests, medicine, and procedures for patients electronically, thus reducing errors associated with hand-written orders and prescriptions.
- Telehealth is used to provide health care to rural and remote areas through the use of communications technologies.
- Personal health records (PHR), like EMRs, are Internet-based and designed to provide access to important health-related information about patients. Unlike EMRs, however, PHRs would be used by the patient and would include additional information provided by the patient not found in the EMR, such as when a prescription was filled.

Due the cost savings and health benefits of HIT, 72 percent of Americans support the creation of a national health information network.*4* However, according to the Department of Health and Human Services (HHS), only a small number of U.S. health care providers have fully adopted HIT as there are significant financial, technical, cultural, and legal barriers to its adoption. Respondents to a recent survey conducted by the Medical Group Management Association reported that only 31 percent of physician group practices use fully operational EHRs.*5* The Healthcare Information and Management Systems Society reported that 19 percent of hospitals use fully operational EHRs. According to a study by the Commonwealth Fund, approximately 13 percent of solo physicians have adopted some form of EHR, while 57 percent of large group practices (50 or more physicians) have adopted an EHR.*6*

On April 27, 2004, President Bush called for widespread adoption of interoperable electronic health records within 10 years and issued an executive order that established the position of the National Coordinator for Health Information Technology. The National Coordinator is to develop and implement a strategic plan to guide the nationwide implementation of interoperable health IT in both the public and private sectors. Two months later, HHS released *The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care—Framework for Strategic Action.* The framework describes actions to be taken by the public and private sectors to develop and implement a strategy that is built on already-existing work in HIT. The framework defines goals and strategies that are to be implemented in three phases. HHS is in the initial phase of implementing activities of the framework by coordinating federal HIT efforts across the government and reaching out to private industry. The framework also introduced the concept of regional health information organizations, which are considered an essential element in the establishment of a national health information network. Regional health information organizations — entities that enable the

---

4 Markle Foundation, Connecting for Health, "Attitudes of Americans Regarding Personal Health Records and Nationwide Electronic Health Information Exchange," October 11, 2005.
5 Government Accountability Office, Health and Human Services' Estimate of Health Care Cost Savings Resulting from the Use of Information Technology, February 16, 2005, GAO-05-309R.
6 Robert Wood Johnson Foundation, "Health Information Technology in the United States: The Information Base for Progress," 2006.

exchange and use of health information — are expected to facilitate information exchange across different jurisdictions and hospital systems.

Other federal agencies also play an important role in fostering the adoption of HIT. The Department of Veterans Affairs — one of the country's largest health care providers — has had an automated information system in its medical facilities since 1985. VA currently uses the Veterans Information Systems & Technology Architecture (VistA), HealthePeople-VistA, the Computerized Patient Record System (CPRS), the Bar Code Medication Administration System, telehealth and VistA Imaging technologies, and the My HealtheVet personal health record.

DoD has provided IT support to its hospitals and clinics since 1968. The Composite Health Care System (CHCS), deployed in 1993, is the primary medical information system now used in all military health system facilities worldwide. In 1997, DoD initiated the Armed Forces Health Longitudinal Technology Application, it will eventually replace CHCS.

In 1998, following a presidential call for VA and DoD to start developing a comprehensive, life-long medical record for each service member, the two departments began a joint course of action aimed at achieving the capability to share patient health information for active duty military personnel and veterans. DoD and VA are still working today to develop a joint EHR.*7*

The Office of Personnel Management (OPM) has responsibility for the Federal Employees Health Benefit Program (FEHBP), which is one of the largest employer-based health insurance programs in the country. OPM is planning to use its leverage as one of the largest purchasers of employee health care benefits to contribute to the expansion and use of EHRs, electronic prescribing, and other HIT-related provisions. OPM is represented on the American Health Information Community (AHIC) and, according to OPM officials, is holding informal discussions with staff from the Office of the National Coordinator. In July 2004, OPM outlined various options for health plans in the FEHBP, such as adopting systems based on generally accepted and certified standards. The 2005 annual Call Letter to carriers requested that plans describe their HIT initiatives, including any currently in place for doctors and pharmacies to use electronic prescribing. According to GAO, OPM received responses from participating health plans and reviewed them to establish a baseline with the intention of measuring progress on the use of HIT.*8*

PRIVACY CONCERNS

Despite the benefits of HIT, there are potential risks. Survey data has demonstrated that consumers are afraid that broader sharing of their personal health information will only make it more vulnerable to unwanted and unintended exposure. In 2003, the Markle Foundation released a survey which revealed that 91 percent of its respondents were very concerned about the privacy of their personal health records. A Harris Interactive survey in February 2005, entitled *How the Public Sees Health Records and an EMR Program*, showed that 70 percent of Americans were

---

7 Daniel Pullman, "VA and Defense Agree to Build Joint Electronic Health System," GovExec.com, January, 24, 2007.
8 Supra note 1.

concerned that an electronic medical records systems would lead to sensitive medical records being exposed due to weak electronic security.

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA), which, among other things, instructed the Secretary of HHS to issue privacy regulations in the event that Congress failed to do so in two years. After this deadline passed without congressional action, HHS issued medical privacy regulations that went into effect on April 14, 2001. The HIPAA Privacy Rule establishes privacy protections for individually identifiable health information held by covered entities (health care providers, health care plans, and health care clearinghouses). It establishes a series of regulatory permissions for uses and disclosures of individually identifiable health information.9 The rule excludes education records and employment records held by a covered entity in its role as employer.

Subsequent to the Privacy Rule, HHS issued the HIPAA Security Rule on February 20, 2003 to safeguard electronic protected health information. The Security Rule includes administrative, physical, and technical safeguards and specific implementation instructions, some of which are required to be implemented by covered entities.

The HIPAA Privacy Rule and the Security Rule provide a foundation for the development of EHR systems; however, the HIPAA rules do not address issues associated with the development of a system in which personal health information is shared electronically across a spectrum of entities that would be involved in the national health information network. For example, some of the companies now offering PHR services do not meet the definition of a covered entity and are not regulated by the HIPAA Privacy Rule.

GAO'S REPORT

Out of concern for the privacy and security federal employees' and all Americans' health information, Senator Akaka and Senator Kennedy asked GAO to review HHS's efforts to ensure privacy as part of its national strategy and to identify challenges associated with protection electronic personal health information. In conjunction with this hearing, the GAO will release its report: "Health Information Technology: Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy."

GAO identifies key challenges associated with protecting personal health information. Below is a description of those challenges:

- Understanding and resolving legal and policy issues, including understanding and resolving data sharing issues introduced by varying state privacy laws and organization-level practices.

---

9 Individually Identifiable Health Information — health information created or received by a covered entity that (A) relates to past, present, or future physical or mental health or a condition of an individual; (B) relates to the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (C) identifies the individual or there is a reasonable basis to believe that the information can be used to identify the individual.

- Ensuring appropriate disclosure, including determining the minimum data necessary that can be disclosed in order for requesters to accomplish their intended purpose. Also, educating consumers about the extent to which their consent to use and disclose heath information applies.
- Ensuring individuals' rights to request access and amendments to health information.
- Implementing adequate security measures for protecting health information, including implementing proper access controls and maintaining adequate audit trails for monitoring access to health data.

GAO recommends that the Secretary of HHS define and implement a comprehensive national strategy to protect private health information. This approach should: (1) identify milestones for integrating the outcomes of HHS's privacy-related initiates, (2) ensure that key privacy principles are fully addressed, and (3) address key challenges associated with the nationwide exchange of health information.

The Assistant Secretary for Legislation at HHS sent written comments to GAO stating disagreement with GAO's recommendations. HHS also asserted that it has made significant progress in integrating these privacy strategies in that it established a strategic objective to protect consumer privacies and initiated two strategies for meeting their objectives.

HIT LEGISLATION

S. 2247, Federal Employees Health Benefits Program Efficiency Act of 2006, introduced by Senator Obama, which directs each carrier entering into a contract under the FEHBP to offer a health benefits plan to implement an electronic system for efficient and effective adjudication of all medical claims and requires that such system be used to monitor for fraud and abuse as part of such adjudication.

S. 3846, Federal Employees Electronic Personal Health Records Act of 2006, introduced by Senators Carper and Voinovich, that amends federal civil service law to require each contract between OPM and a qualified carrier offering a health benefit plan for federal employees to provide for establishment and maintenance of electronic personal health records for each individual and family member enrolled in the plan. Directs OPM to ensure that each individual and family member is given an opportunity to elect at any time to opt out of participation in the record program or terminate an established record.

H.R. 4859, Federal Family Health Information Technology Act of 2006, introduced by Representative Jon Porter, that sets forth provisions concerning the establishment of a system of electronic health records for covered individuals under the FEHBP. Directs that each contract under FEHBP shall require that the carrier establish, maintain, and make available a carrier electronic health record for each covered individual who is enrolled under FEHBP in a health benefits plan offered by such carrier.

S. 1418, Wired for Health Care Quality Act, introduced by Senator Enzi, that would promote the development of a nationwide interoperable health information technology infrastructure.

H.R. 4157, Health Information Technology Promotion Act of 2006, introduced by Representative Nancy Johnson, to promote better health information systems.

ADDITIONAL INFORMATION

Executive Order 13335, *Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator* (Washington, D.C.: April 27, 2004).

The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care—Framework for Strategic Action
HTTP://WWW.HHS.GOV/HEALTHIT/FRAMEWORKCHAPTERS.HTML

The Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Federal Financial Management, Government Information, and International Security held a hearing during the 109th Congress on June 22, 2006 entitled, *Lessons Learned? Assuring Healthy Initiatives in Health Information Technology.*

The House Committee on Government Reform, Subcommittee on the Federal Workforce and Agency Organization held a hearing during the 109th Congress on March 15, 2006 entitled, *Healthier Feds and Families: Introducing Information Technology into the Federal Employees Health Benefits Program.*

The House Committee on Government Reform, Subcommittee on the Federal Workforce and Agency Organization held a hearing during the 109th Congress on July 27, 2005 entitled, *Is There a Doctor in the Mouse? Using Information Technology to Improve Health Care.*

The House Committee on Government Reform held a hearing during the 109th Congress on September 29, 2005 entitled, *The Last Frontier: Bringing the it Revolution to Healthcare.*

The Health Privacy Project. http://www.healthprivacy.org

Government Accountability Office, *Health Information Technology: HHS Is Taking Steps to Develop a National Strategy, May 2005*, GAO-05-628

The Markle Foundation. http://www.markle.org/markle_programs/healthcare/index.php

Testimony Before the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia

Private Health Records: Privacy Implications of the Federal Government's Health Information Technology Initiative

Statement of

Robert Kolodner, M.D.

Interim National Coordinator,
Office of the National Coordinator for Health IT
U.S. Department of Health and Human Services

February 1, 2007

Chairman Akaka and Senator Voinovich, thank you for inviting me to testify today to discuss the Department of Health and Human Services (HHS) national health information technology (health IT) agenda and our approach to assuring that electronic personal health information is secure and protected.

Introduction

On April 27, 2004, the President signed Executive Order 13335 announcing his commitment to the promotion of health IT to improve efficiency, reduce medical errors, improve quality of care, and provide better information for patients and physicians. At that time, the President also called for widespread adoption of electronic health records (EHRs) by 2014 so that health information will follow patients throughout their care in a seamless and secure manner. Reaching this ambitious goal requires cooperation among Federal agencies and Departments that play a role in advancing our understanding and use of health information technology: coordination across all Federal health IT programs; and coordination with the private sector. Toward those ends, the President directed the Secretary of HHS to establish within his office the position of National Coordinator for Health Information Technology to advance this vision.

Moreover, on August 22, 2006, the President issued Executive Order 13410 to ensure that health care programs administered or sponsored by the Federal Government promote quality and efficient delivery of health care through the use of interoperable health IT, transparency regarding health care quality and price, and better incentives for program beneficiaries, enrollees, and providers. The Executive Order further advances movement towards a modern health information system by directing, to the extent permitted by law, that "[a]s each agency implements, acquires, or upgrades health information technology systems used for the direct exchange of health information between agencies and with non-Federal entities, it shall utilize, where available, health information technology systems and products that meet recognized interoperability standards."

HHS has established and is pursuing a deliberative, comprehensive, and integrated approach to ensure the privacy and security of health information within a nationwide health IT infrastructure. HHS is on track to improve quality of care through adoption of interoperable health IT while concurrently providing solid protection of health information. We continue to implement a "Framework for Strategic Action," initially articulated in July 2004, which serves as a foundational guide for nationwide health IT adoption. Safeguarding personal health information is essential to our national strategy for health IT and a strategy devoid of measures to ensure privacy and security would neither advance our interests nor those of the American people. The Office of the National Coordinator for Health Information Technology (ONC) is responsible for HHS' strategic plan for the nationwide implementation of interoperable health IT, including the integration of privacy-related health IT initiatives. ONC anticipates delivering a draft strategic plan to the Secretary's office in 2007 that both integrates our understanding and knowledge from 2005 and 2006 activities and provides direction to meet the President's 2014 goal.

HHS's strategy recognizes the importance of collaboration with both the public and private sectors, including representation from consumers of health care services. Many of our activities

rely on public input, recommendations from Federal advisory committees, and deliverables from contracts with a wide variety of health care and IT sector collaborators, among other sources. Nationwide health IT adoption can only be accomplished through the coordinated effort of many stakeholders, within both state and Federal governments and the private sector. HHS has taken great care to engage representatives of all these sectors in our many health IT initiatives – an effort that involves many processes and the work of thousands of participants.

Health Information Privacy and Security

Personal health information is sensitive, and patients and providers are genuinely interested in assuring that it is adequately protected.

When protecting Federal information, including Personally Identifiable Information and health information, the Government already has a robust framework in place and numerous policies related to the privacy and security of information, including but not limited to: requirements set forth in the Federal Information Security Management Act (FISMA), the Privacy Act, Office of Management and Budget policies, and guidance and standards put forth by the National Institute of Standards and Technology (NIST). For example, under FISMA, government information (including health information and personally identifiable information) is required to be categorized and protected based on the level of risk associated with that information. Guidance documents and standards exist for agencies to follow - requiring minimum technical, operational, and management controls.

Beyond the Federal government, health care providers have had policies in place to protect the privacy of their patients long before the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. HHS has promulgated several rules that establish critical foundations of Federal confidentiality, privacy, and security protections for health information across the health care system, including the HIPAA Privacy Rule, the HIPAA Security Rule, the HIPAA enforcement rule, and the regulation on Confidentiality of Alcohol and Drug Abuse Patient Records Regulation. Taken together, these Rules establish the foundational principles of, and form the context for, the comprehensive privacy and security approach HHS continues to take as part of our national health IT agenda. Furthermore, HHS believes the current HIPAA statute provides an appropriate amount of flexibility to protect health information in the health IT environment while allowing best practices to emerge. There are differences between Federal laws, State laws and business practices. Sometimes, these differences provide additional challenges for secure sharing of health information in a private and secure manner, an issue that is currently being examined.

While we may not be able to prevent every improper disclosure of health information, the number, type, and sophistication of tools to protect electronic information are growing at an ever-increasing rate and provide the opportunity to offer health privacy protections beyond those in the paper environment. For example, implementation of role-based access controls and auditing, when implemented electronically, can limit access to a patient's record to only those individuals who need the information for treatment. Audit trails can automatically record who viewed the health record and can be used after the fact to identify any unauthorized access, leading to improvements in training or, if warranted, corrective action.

The change toward electronic health records will not only save lives and reduce waste, but will also create both new challenges and new opportunities with respect to protecting health information. HIPAA created a strong foundation of privacy and security protections for personal health information upon which States may provide additional privacy protections. HHS is very committed to privacy and security as it works toward the President's goal of widespread interoperable electronic health records. Ultimately, the effective coordination of health IT activities will help create an environment in which the health status of the American public is improved and its confidentiality and privacy are secure.

Ensuring Privacy and Security Protections through Health IT

HHS has invested significant resources and efforts in our nationwide strategy for protecting health information. Our national health IT agenda approaches privacy and security through a full suite of activities that both inform current work and prepare for future needs. We are leveraging existing foundations; creating new public-private collaborations; partnering with states, health care organizations, and consumers to address state and business level protections; and considering privacy and security policies and implementation at a nationwide level.

Privacy and Security Solutions for Interoperable Health Information Exchange
The Privacy and Security Solutions contract awarded to RTI International (RTI), co-managed by ONC and the Agency for Healthcare Research and Quality (AHRQ), has fostered an environment for states and territories to: (1) assess variations in organization-level business policies and state laws that affect health information exchange; (2) identify and propose practical solutions, while preserving the privacy and security requirements in applicable Federal and state laws; and (3) develop detailed plans to implement solutions to identified privacy and security challenges. States and territories – through the participation of many volunteer stakeholders including physicians, pharmacists, consumers, health IT vendors, laboratories, attorneys, insurers, etc. – have focused their work on an analysis of eighteen health information exchange scenarios which expose challenges their state or territory may face in an electronic environment. The scenarios which touch on issues such as treatment, payment, research, and bioterrorism, provided states and territories a framework within which to map their variations in business practices and policies to the nine supplied "domains" of privacy and security:

- user and entity authentication;
- authorization and access control;
- patient and provider identification;
- transmission security;
- information protection;
- information audits;
- administrative and physical safeguards;
- state law; and
- use and disclosure policy.

The 34 states and territories that are part of the Health Information Security and Privacy Collaboration (HISPC) under the Privacy and Security Solutions contract participated in ten regional meetings in the fall of 2006 where they exchanged thoughts with regional counterparts

and discussed the appearance of common themes such as misinterpretations of HIPAA, state consent laws, and the protection variations states provided to specific disease information, such as HIV/AIDS. In November 2006, the HISPC states and territories submitted their interim assessment of variation reports to RTI and will complete the remainder of their work this spring, including several other interim and final reports. In April 2007, the states and territories will advance implementation plans that will not only inform health information exchange initiatives in the states and territories that created them, but will serve as input to other ONC-coordinated efforts such as the State Alliance for E-Health's Health Information Protection taskforce.

State Alliance for E-Health
ONC contracted with the National Governors Association Center for Best Practices to create the State Alliance for e-Health (State Alliance). The State Alliance is an initiative designed to improve the nation's health care system through the formation of a collaborative body that brings together key state decision makers. This body, led by Governors and other high-level executives of states and U.S. territories will be charged with: (1) identifying, assessing and, through the formation of consensus solutions, mapping ways to resolve state-level health IT policy issues that affect multiple states and pose challenges to interoperable electronic health information exchange; (2) providing a forum in which states may collaborate so as to increase the efficiency and effectiveness of the health IT initiatives that they develop; and (3) focusing on privacy and security policy issues surrounding the use and disclosure of electronic health information. The Health Information Protection taskforce, tasked with examining these privacy and security issues, will serve as a catalyst for states and territories to develop uniformity in their health IT privacy and security practices, where appropriate, while preserving or developing privacy and security protections for electronic health information.

Development of Best Practices for State HIE Initiatives
ONC has awarded a contract to the Foundation of Research and Education (FORE) of the American Health Information Management Association (AHIMA) to gather information from existing state-level Health Information Exchanges and define, through a consensus-based process, best practices, including privacy and security practices, that can be disseminated across a broad spectrum of health care and governmental organizations. FORE derived the information from health information exchange policies and other sources on governance, legal, financial and operational characteristics, and health information exchange policies. From their findings, they developed guiding principles and practical guidance for state-level health information exchanges. AHIMA also developed a workbook and final report to disseminate guiding principles, and recommendations on how to encourage conformance and coordination across state and federal initiatives.

American Health Information Community: Confidentiality, Privacy, and Security (CPS) Workgroup
In September 2005, the Secretary established the American Health Information Community (AHIC), a federally-chartered advisory committee made up of key leaders from the public and private sectors, charged with making recommendations to HHS on key health IT strategies. In the summer of 2006, the AHIC on the basis of a recommendation issued jointly by three of its workgroups (Chronic Care, Electronic Health Records, Consumer Empowerment) created a workgroup specifically focused on nationwide privacy and security issues raised by health IT

activities and the findings of the other AHIC workgroups – privacy and security are one of the most consistent threads between each of the groups and their breakthrough projects. The workgroup members were carefully selected to assure that there was sufficient privacy and security expertise, sufficient consumer input, and representation of relevant health care stakeholders that may be affected by any recommendations developed. The workgroup's first set of recommendations on patient identity proofing were advanced and accepted after deliberation by the AHIC on January 23, 2007, for recommendation to the Secretary of HHS. These recommendations, if adopted by HHS and others, together with existing protections, will inform the AHIC's breakthrough activities and serve as a model for the private sector in this area. The workgroup is currently prioritizing its next issue and is contemplating a privacy focused discussion in collaboration with the Consumer Empowerment workgroup on the personal health record (PHR) environment and associated privacy protections.

American Health Information Community: Personalized Healthcare Workgroup
One of Secretary Leavitt's top priorities is the personalized health care initiative that aims to improve the quality and effectiveness of health care at a personal level. The major tenets of the initiative are to improve the development of information about each individual's health and disease states based on genomic medical testing and to support the proper use of this information. Individualized approaches to health care are feasible because of improvements in the scientific knowledge about the genetic and environmental associations of disease, improvements in technologies to determine genetic alterations responsible for disease, and health information technologies to support knowledge development and patient care.

Formed in December 2006, the Personalized Healthcare workgroup of the AHIC is specifically charged to make recommendations to the AHIC, designed to facilitate the inclusion of genomic medical test information and family history information into EHRs. The AHIC requested that this workgroup work collaboratively with the Confidentiality, Privacy, and Security workgroup to address issues such as non-discrimination, de-identification, and secondary uses, associated with genomic test information in EHRs. The Personalized Healthcare workgroup has a robust, experienced membership consisting of experts from academia, the Federal government and industry, and will be working to address the concerns expressed above and present recommendations to the AHIC.

The Certification Commission for Healthcare Information Technology (CCHIT)
In September 2005, ONC directed CCHIT to advance the adoption of interoperability standards and reduce barriers to the adoption of interoperable health information technologies through the creation of an efficient, credible and sustainable product certification program. The CCHIT membership includes a broad array of private sector representatives, including physicians and other health care providers, payers and purchasers, health IT vendors, and consumers. An important part of CCHIT's work is to set criteria for, and certify the security of, health information systems. CCHIT has done this for ambulatory EHR systems with the definition of twenty-nine security criteria that EHRs had to meet to achieve certification in 2006.

Through January 2007, CCHIT has certified 55 ambulatory EHRs that meet these security criteria among others for functionality and interoperability. In 2007 and 2008, the CCHIT will develop security criteria to certify inpatient EHR systems and network services. In addition,

CCHIT updates previously published certification criteria on an annual basis, and as a result, additional security criteria for ambulatory EHRs were added for the 2007 round of testing. The certification process CCHIT has developed promotes well-established, tested, security capabilities in health IT systems and helps make certification a major contributor to protecting the privacy and confidentially of the data these systems manage.

Healthcare Information Technology Standards Panel (HITSP)
Pursuant to a contract with ONC, the American National Standards Institute (ANSI) convened the HITSP in September 2005, to identify standards for use in enhancing the exchange of interoperable health data. The process carried out by HITSP has created a unique and unprecedented opportunity to bring together the intellectual assets of over 260 organizations with a stake in health data standards that will increase the interoperability of health care systems and information.

A part of the HITSP mission is to harmonize the standards necessary to allow for the protection of the privacy and security of health data. The panel guides the collaboration of its member organizations through a standards harmonization process that leverages the work and membership of multiple standards development organizations along with the expertise from the public and private sector. The panel engages in a consensus-based process to identify the most appropriate standards, to identify gaps in standards where they are inadequate or unavailable and specifies the use of those standards to advance interoperability. HITSP ensures that concerns of interested parties are appropriately addressed and resolved, that the proceedings remain open to the public, that the industry's interests are adequately balanced, and further, that interested parties are given ample opportunities to give input to technical committee and panel decisions.

HITSP identifies standards and guidance to support specific clinical use-cases, and has developed a special working group and focus for security related standards for 2007. On October 31, 2006, HITSP presented and the AHIC accepted and subsequently recommended to the Secretary, three "Interoperability Specifications" that include 30 consensus standards and over 800 pages of implementation guidance for recommendation to HHS. The Secretary has since accepted these Interoperability Specifications, which he anticipates recognizing in December 2007, and HITSP will now move on to harmonize standards in four new AHIC-prioritized areas (Emergency Responder EHR, Quality, Patient Access to Clinical Information, Medication Management).

Nationwide Health Information Network (NHIN)
In November 2005, ONC awarded contracts to four consortia to develop prototypes capable of demonstrating potential solutions for nationwide exchange of health information. This initiative is foundational to the President's vision for the widespread adoption of secure, interoperable health records within 10 years. The prototype architectures developed provide a framework for a public-private discussion on needed capabilities to support secure health information exchange across the nation. Each contract includes three geographically distinct health care markets. The output of the NHIN initiative includes prototype architectures that include functional requirements, business models, the identification of needed standards, and prototype software implementations. It is anticipated that the NHIN will leverage the existing internet infrastructure in a "network of networks" architectural model, allowing existing health information exchanges

to participate, as well as other providers who are not currently actively involved in health information exchange.

In anticipation of this initiative, among others, the National Committee on Vital and Health Statistics (NCVHS), (an advisory committee to the Secretary that was established in 1949 and charged by Congress with advising the federal government on the information needs underlying health policy) had already begun a series of hearings on privacy and the NHIN. Based on these hearings, NCVHS submitted findings and recommendations to HHS in June 2006 in the report, *Privacy and Confidentiality in the Nationwide Health Information Network.* We are in the processing of considering the recommendations in that report. In the meantime, NCVHS continues to refine its work in this area.

In late spring 2006, ONC asked NCVHS to recommend a minimum, but inclusive, set of functional requirements necessary for nationwide health information activities. To undertake this task, NCVHS utilized an open process through which they received significant public comment. NCVHS participated in the NHIN Forums on June 28-29 and October 16-17, 2006; held public hearings on June 29 and July 27-28, 2006, in Washington, DC; and held public conference calls on August 31 and October 3, 2006 to receive comments on preliminary documents and drafts. The process used to develop recommendations for the set of high level functional requirements included an analysis of the original 977 detailed functional requirements, followed by a consolidation of those 977 requirements into a working set of minimum but inclusive set of functional requirements, and then a refinement of the working set into high level functional requirements. The final high level set of functional requirements touched on certification, authentication, authorization, person identification, location of health information, transport and content standards, data transactions, auditing and logging, time-sensitive data access, communications, and data storage.

A critical portion of the required NHIN deliverables is the development of security models that directly address systems architecture needs for securing and maintaining the confidentially of health data. The NHIN prototypes included the development of architecture that would provide consumers with the ability to manage disclosures of their electronic health information. Furthermore, each participant is required to comply with security requirements established by HHS and Federal laws, where applicable, to ensure proper and confidential handling of data and information. Each is delivering important architecture capabilities that will be used in the next steps of the NHIN to address the complex issues of authentication, authorization, data access restrictions, auditing and logging, consumer controls of information access and other critical contributions.

Conclusion

Privacy and security policies and their associated technological solutions cannot be developed in a vacuum. A key component to assure that appropriate privacy and security protections are in place is to assure that these efforts develop in tandem and that coordination is consistent throughout these efforts. This is the role of ONC. We have a conscientious, experienced, and passionate staff that works closely together on these activities and other privacy and security related activities throughout HHS and the other Departments and Agencies to ensure that health

IT policy decisions and technology solutions are appropriately coordinated and addressed. ONC is currently working to ensure that the AHIC CPS workgroup works collaboratively with the NCVHS to address the challenges posed by secondary uses of health information in the electronic environment including those related to non-HIPAA covered entities.

HHS has made considerable progress integrating the activities and processes listed above into our overall strategy for ensuring privacy and security protections for health information in a health IT infrastructure. Each activity and process involves many participants and organizations and will play a critical role in ensuring privacy and security of health information while advancing the adoption of health IT. Each activity and process has numerous deliverables and milestones. Many of our initiatives involve complex collaborative efforts and HHS seeks to be responsive to public comments and concerns while coordinating these public-private initiatives. HHS is focused directly on these privacy and security policy issues and is coordinating the integration of these policy issues through the health IT technology efforts presented.

Mr. Chairman, thank you for the opportunity to appear before you today.

STATEMENT OF
DANIEL A. GREEN
DEPUTY ASSOCIATE DIRECTOR
CENTER FOR EMPLOYEE AND FAMILY SUPPORT POLICY
STRATEGIC HUMAN RESOURCES POLICY
OFFICE OF PERSONNEL MANAGEMENT

before the

SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT MANAGEMENT, THE FEDERAL WORKFORCE, AND THE DISTRICT OF COLUMBIA
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

on

Private Health Records: Privacy Implications of the Federal Government's Health Information Technology Initiative

February 1, 2007

Mr. Chairman and Members of the Subcommittee:

It is a pleasure to be here today to represent Director Linda Springer and to discuss how OPM is working with the Department of Health and Human Services (HHS), other Federal Agencies, and Public/private bodies to ensure that security and privacy are an integral part of the national health information technology (HIT) initiative. In his State of the Union address, President George W. Bush voiced his support for better information technology and he further stated that "In all we do, we must remember that the best health care decisions are made not by government and insurance

companies, but by patients and their doctors." I am here today to describe how we are working to carry out the President's objectives and to ensure that the privacy rights of our Federal healthcare consumers are protected.

Administering the Federal Employees Health Benefit Program

OPM administers the Federal Employees Health Benefits (FEHB) Program, which covers approximately 8 million Federal employees, retirees and their dependents. FEHB offers competitive health benefits products for Federal workers, much like large employer purchasers in the private sector, by contracting with private sector health plans. OPM has consistently encouraged participating health plans to be responsive to consumer interests by emphasizing flexibility and consumer choice as key features of the program. We have also encouraged plans to adopt health information technology as another important consumer oriented initiative. At the same time, we have stressed that the privacy and security of individual health information is of paramount importance.

FEHB enrollees have the same privacy protections under Federal law as all Americans. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides for the adoption of standards for health care transactions and the protection of the privacy of individually identifiable health information. All FEHB health carriers are required to be in compliance with HIPAA requirements. And, if there are any other Federal

laws enacted which apply to our carriers and similarly protect the privacy of personal health information, we will expect compliance.

HIT, Privacy and the FEHB Program

OPM has been very active in the area of health information technology. In 2004, President George W. Bush, by way of Executive Order 13335, clearly established the importance of the development and implementation of a nationwide interoperable health information technology (HIT) infrastructure to improve the quality and efficiency of health care. The Executive Order also required patients' individually identifiable health information to be secure and protected. As the administrator of the country's largest employer-sponsored health insurance programs, OPM plays a key role in fulfilling President Bush's vision of making health information easily accessible to consumers through the adoption of advanced technologies.

In response to the Executive Order, we submitted a report to President Bush in July 2004 that outlined possible options OPM could take to facilitate the nationwide adoption of interoperable HIT. Early in 2005, we issued our annual FEHB "Call Letter" to provide guidance and negotiation objectives for benefit and rate proposals from FEHB Program plans for the next contract term. In that letter, we encouraged FEHB plans to begin making focused efforts toward the greater use of HIT while ensuring compliance with Federal requirements to protect the privacy and security of personal

health information. We found that, while there were wide variations in the scope and extent of HIT use, most plans were focusing their efforts on providing claims-based information through their web sites, linking disease management programs to HIT initiatives, and e-Prescribing. Since that time, some plans have developed robust HIT systems and we are recognizing their efforts on OPM's website. We will discuss these efforts in more detail shortly.

In September 2005, the American Health Information Community (the Community) was formed. It is chaired by the Secretary of Health and Human Services (HHS), Mike Leavitt, as a Federally-chartered advisory committee charged with developing recommendations for HHS on key health IT strategies. Secretary Leavitt named Director Springer as a member of the Community. OPM employees serve on the Consumer Empowerment Workgroup. The workgroup has a broad charge to make recommendations to the Community to gain widespread adoption of a personal health record that is easy-to-use, portable, longitudinal, affordable, and consumer-centered.

OPM employees also serve on the Quality Workgroup. This workgroup has a broad charge to make recommendations to the Community so that HIT can provide the data needed for the development of quality

measures and to make recommendations on how performance measures should align with the capabilities and limitations of health IT.

Another workgroup formed by the Community is the Confidentiality, Privacy and Security Workgroup. As a Community member, we remain informed of its activities and recommendations. We will continue to closely monitor the workgroup's activities. When their recommendations are presented to the Community, we will evaluate them for applicability to FEHB carrier contracts.

OPM is also a member of the interagency Health IT Policy Council. This Council was established to coordinate Federal health information technology policy decisions across Federal Departments and agencies that will drive Federal action necessary to realize the President's goals of widespread health IT adoption.

In 2006, our call letter asked FEHB carriers to work toward several specific short-term objectives. These included enhancing educational efforts to increase awareness of the value of HIT among plan members; offering personal health records to consumers based on their medical claims history; encouraging ePrescribing; and linking disease management programs with HIT systems. Again, we stressed the need to ensure compliance with

Federal requirements to protect the privacy and security of individually identifiable health information.

We highlighted those FEHB plans with state-of-the-art HIT capabilities on our website during the November 2006 Open Season so that consumers would have this additional information to take into consideration in making their plan choices.

In August of 2006, President Bush issued Executive Order 13410, *Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs*. It underscored the President's continued commitment to the promotion of quality and efficient delivery of health care. With the Order, the President greatly expanded the information about FEHB plans to be made available to Federal employees and committed the Federal Government to transparency in pricing and, quality, implementation of health IT interoperability standards, and insurance options that reward cost-conscious consumers.

In support of the Order, OPM has required all FEHB plans to report on quality measures, including data from the Health Plan Employer Data and Information Set. OPM has also encouraged all plans to provide information on cost and quality transparency. Along with the plans with state-of-the-art HIT capabilities, this additional information was prominently positioned on OPM's Open Season website to assist prospective enrollees with making

informed health plan choices for 2007. Last, and most important, OPM has informed carriers they must continue to ensure compliance with Federal requirements that protect the privacy and security of individually identifiable health information.

Looking forward, OPM will require, to the extent permitted by law, FEHB carriers to adopt standards for interoperability of health information records in harmony with their adoption and implementation in the healthcare industry. And, we will continue to expand the FEHB web site to provide information regarding carriers' cost and quality transparency initiatives, as well as their health IT capabilities, so prospective enrollees can view the information in making their health plan choices for 2008.

The FEHB Program has always been a market-based program and relies on competition to provide choice and to keep costs reasonable. Along these lines, we are encouraging FEHB plans to continue offering insurance options that reward consumers for choices based on quality and cost. And, we will continue to focus efforts on accelerating the use of HIT to further the President's goals.

We firmly believe privacy and security of personal health information is important. We are encouraged by HHS' efforts to address this important issue. We plan to continue to work closely with HHS, the Community and

the HIT Policy Council to ensure all necessary steps are taken to protect consumer privacy rights.

We appreciate this opportunity to testify before the Subcommittee on this very important issue. I will be glad to answer any questions you may have.

United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia; Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 2:30 p.m. EST
Thursday, February 1, 2007

HEALTH INFORMATION TECHNOLOGY

Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy

Statement of
Linda D. Koontz
Director, Information Management Issues

David A. Powner
Director, Information Technology Management Issues

GAO
Accountability * Integrity * Reliability

GAO-07-400T

Abbreviations

AHIC	American Health Information Community
Health IT	health information technology
HIPAA	Health Insurance Portability and Accountability Act of 1996
HHS	Health and Human Services
NCVHS	National Committee on Vital and Health Statistics
NHIN	Nationwide Health Information Network

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

February 2007

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-07-400T, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

HEALTH INFORMATION TECHNOLOGY

Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy

Why GAO Did This Study

In April 2004, President Bush called for the Department of Health and Human Services (HHS) to develop and implement a strategic plan to guide the nationwide implementation of health IT. The plan is to recommend methods to ensure the privacy of electronic health information.

GAO was asked to summarize its report that is being released today. The report describes the steps HHS is taking to ensure privacy protection as part of its national health IT strategy and identifies challenges associated with protecting electronic health information exchanged within a nationwide health information network.

What GAO Recommends

GAO recommended that HHS define and implement an overall privacy approach that identifies milestones for integrating the outcomes of its initiatives, ensures that key privacy principles are fully addressed, and addresses challenges associated with the nationwide exchange of health information. In its comments, HHS disagreed with this recommendation and stated that it has established a comprehensive privacy approach. However, GAO believes that an overall approach for integrating HHS's initiatives has not been fully defined and implemented.

www.gao.gov/cgi-bin/getrpt?GAO-07-400T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Linda D. Koontz, (202) 512-6240, koontzl@gao.gov.

What GAO Found

HHS and its Office of the National Coordinator for Health IT have initiated actions to identify solutions for protecting personal health information through several contracts and with two health information advisory committees. For example, in late 2005, HHS awarded several health IT contracts that include requirements for addressing the privacy of personal health information exchanged within a nationwide health information exchange network. Its privacy and security solutions contractor is to assess the organization-level privacy- and security-related policies, practices, laws, and regulations that affect interoperable health information exchange. Additionally, in June 2006, the National Committee on Vital and Health Statistics made recommendations to the Secretary of HHS on protecting the privacy of personal health information within a nationwide health information network and in August 2006, the American Health Information Community convened a work group to address privacy and security policy issues for nationwide health information exchange. While these activities are intended to address aspects of key principles for protecting the privacy of health information, HHS is in the early stages of its efforts and has therefore not yet defined an overall approach for integrating its various privacy-related initiatives and addressing key privacy principles, nor has it defined milestones for integrating the results of these activities.

GAO identified key challenges associated with protecting electronic personal health information in four areas (see table).

Challenges to Exchanging Electronic Health Information

Areas	
Understanding and resolving legal and policy issues	• Resolving uncertainties regarding the extent of federal privacy protection required of various organizations • Understanding and resolving data sharing issues introduced by varying state privacy laws and organization-level practices • Reaching agreements on differing interpretations and applications of the HIPAA privacy and security rules • Determining liability and enforcing sanctions in case of breaches of confidentiality
Ensuring appropriate disclosure	• Determining the minimum data necessary that can be disclosed in order for requesters to accomplish their intended purposes • Determining the best way to allow patients to participate in and consent to electronic health information exchange • Educating consumers about the extent to which their consent to use and disclose health information applies
Ensuring individuals' rights to request access and amendments to health information	• Ensuring that individuals understand that they have rights to request access and amendments to their own health information • Ensuring that individuals' amendments are properly made and tracked across multiple locations
Implementing adequate security measures for protecting health information	• Determining and implementing adequate techniques for authenticating requesters of health information • Implementing proper access controls and maintaining adequate audit trails for monitoring access to health data • Protecting data stored on portable devices and transmitted between business partners

Source: GAO analysis of information provided by state-level health information exchange organizations, federal health care providers, and health IT professional associations.

Mr. Chairman, Senator Voinovich, Members of the Subcommittee:

We appreciate the opportunity to participate in today's hearing on privacy initiatives associated with the Department of Health and Human Services's (HHS) national health information technology (IT) strategy. Key privacy principles for protecting personal information have been in existence for years and provide a foundation for privacy laws, practices, and policies. Those privacy principles are reflected in the provisions of the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, which define the circumstances under which an individual's protected health information may be used or disclosed.

In April 2004, President Bush issued an executive order that called for the development and implementation of a strategic plan to guide the nationwide implementation of interoperable health IT in both the public and private sectors.[1] The plan is to address privacy and security issues related to interoperable health IT and recommend methods to ensure appropriate authorization, authentication, and encryption of data for transmission over the Internet. The order also established the position of the National Coordinator for Health Information Technology within HHS as the government official responsible for developing and implementing this strategic plan.

As requested, our testimony summarizes a report being released today that (1) describes the steps HHS is taking to ensure privacy protection as part of the national health IT strategy and (2) identifies challenges associated with meeting requirements for protecting personal health information within a nationwide health information network.[2] In preparing for this testimony, we relied on our work supporting the report, which contains a detailed overview of our scope and methodology. The work on which this testimony is based

[1]Executive Order 13335, *Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator* (Washington, D.C.: Apr. 27, 2004).

[2]GAO, *Health Information Technology: Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy*, GAO-07-238 (Washington, D.C.: Jan. 10, 2007).

was performed in accordance with generally accepted government auditing standards.

Results in Brief

HHS and its Office of the National Coordinator for Health IT have initiated actions to study the protection of personal health information through the work of several contracts, the National Committee on Vital and Health Statistics,[3] and the American Health Information Community.[4] For example:

- In late 2005, HHS awarded several health IT contracts that include requirements for addressing the privacy of personal health information exchanged within an electronic nationwide health information network.
- In summer 2006, HHS's contractor for privacy and security solutions selected 33 states and Puerto Rico as locations in which to perform assessments of organization-level privacy- and security-related policies, practices, laws, and regulations that affect interoperable health information exchange and to propose privacy and security protections that permit interoperability.
- In June 2006, the National Committee on Vital and Health Statistics provided a report to the Secretary of HHS that made recommendations on protecting the privacy of personal health information within a nationwide health information network.

[3]The National Committee on Vital and Health Statistics was established in 1949 as a public advisory committee that is statutorily authorized to advise the Secretary of HHS on health data, statistics, and national health information policy, including the implementation of health IT standards.

[4]The American Health Information Community is a federally chartered advisory committee made up of representatives from both the public and private health care sectors. The community provides input and recommendations to HHS on making health records electronic and providing assurance that the privacy and security of those records are protected.

- In August 2006, the American Health Information Community also convened a work group to address privacy and security policy issues for nationwide health information exchange.

HHS and its Office of the National Coordinator for Health IT intend to use the results of these activities to identify technology and policy solutions for protecting personal health information as part of their continuing efforts to complete a national strategy to guide the nationwide implementation of health IT. While these activities are intended to address aspects of key principles for protecting health information, HHS is in the early stages of its efforts and has not yet defined an overall approach for integrating its various privacy-related initiatives and addressing key privacy principles. In addition, milestones for integrating the results of these activities do not yet exist. Until HHS defines an integration approach and milestones for completing these steps, its overall approach for ensuring the privacy and protection of personal health information exchanged throughout a nationwide network will remain unclear.

Key challenges associated with protecting personal health information are understanding and resolving legal and policy issues, such as those related to variations in states' privacy laws; ensuring that only the minimum amount of information necessary is disclosed to only those entities authorized to receive the information; ensuring individuals' rights to request access and amendments to their own health information; and implementing adequate security measures for protecting health information.

We recommend in our report that the Secretary of HHS define and implement an overall approach for protecting health information as part of the strategic plan called for by the President. This approach should (1) identify milestones for integrating the outcomes of its privacy-related initiatives, (2) ensure that key privacy principles are fully addressed, and (3) address key challenges associated with the nationwide exchange of health information.

In written comments, HHS disagreed with our recommendation and referred to the department's "comprehensive and integrated approach for ensuring the privacy and security of health information within nationwide health information exchange." However, an

overall approach for integrating the department's various privacy-related initiatives has not been fully defined and implemented. We acknowledge in our report that HHS has established a strategic objective to protect consumer privacy along with two specific strategies for meeting this objective. Our report also acknowledges the key efforts that HHS has initiated to address this objective. While progress has been made initiating these efforts, much work remains before they are completed and the outcomes of the various efforts are integrated. Thus, we recommend that HHS define and implement a comprehensive privacy approach that includes milestones for integration, identifies the entity responsible for integrating the outcomes of its privacy-related initiatives, addresses key privacy principles, and ensures that challenges are addressed in order to meet the department's objective to protect the privacy of health information exchanged within a nationwide health information network.

Background

According to the Institute of Medicine, the federal government has a central role in shaping nearly all aspects of the health care industry as a regulator, purchaser, health care provider, and sponsor of research, education, and training. According to HHS, federal agencies fund more than a third of the nation's total health care costs. Given the level of the federal government's participation in providing health care, it has been urged to take a leadership role in driving change to improve the quality and effectiveness of medical care in the United States, including expanded adoption of IT.

In April 2004, President Bush called for the widespread adoption of interoperable electronic health records within 10 years and issued an executive order that established the position of the National Coordinator for Health Information Technology within HHS as the government official responsible for the development and execution of a strategic plan to guide the nationwide implementation of

interoperable health IT in both the public and private sectors.[5] In July 2004, HHS released *The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care—Framework for Strategic Action.*[6] This framework described goals for achieving nationwide interoperability of health IT and actions to be taken by both the public and private sectors in implementing a strategy. HHS's Office of the National Coordinator for Health IT updated the framework's goals in June 2006 and included an objective for protecting consumer privacy. It identified two specific strategies for meeting this objective—(1) support the development and implementation of appropriate privacy and security policies, practices, and standards for electronic health information exchange and (2) develop and support policies to protect against discrimination based on personal health information such as denial of medical insurance or employment.

In July 2004, we testified on the benefits that effective implementation of IT can bring to the health care industry and the need for HHS to provide continued leadership, clear direction, and mechanisms to monitor progress in order to bring about measurable improvements.[7] Since then, we have reported or testified on several occasions on HHS's efforts to define its national strategy for health IT. We have recommended that HHS develop the detailed plans and milestones needed to ensure that its goals are met and HHS agreed with our recommendation and has taken some steps to define more detailed plans.[8] In our report and testimonies, we have described a number of actions that HHS, through the Office of the National Coordinator for Health IT, has taken toward accelerating the use of

[5]Executive Order 13335.

[6]Department of Health and Human Services, *"The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care: A Framework for Strategic Action"* (Washington, D.C.: July 21, 2004).

[7]GAO, *Health Care: National Strategy Needed to Accelerate the Implementation of Information Technology*, GAO-04-947T (Washington, D.C.: July 14, 2004).

[8]GAO, *Health Information Technology: HHS Is Continuing Efforts to Define Its National Strategy*, GAO-06-1071T (Washington, D.C.: Sept. 1, 2006).

IT to transform the health care industry,[9] including the development of its framework for strategic action. We have also described the Office of the National Coordinator's continuing efforts to work with other federal agencies to revise and refine the goals and strategies identified in its initial framework. The current draft framework—*The Office of the National Coordinator: Goals, Objectives, and Strategies*—identifies objectives for accomplishing each of four goals, along with 32 high-level strategies for meeting the objectives, including the two strategies for protecting consumer privacy.

Health Insurance Portability and Accountability Act of 1996

Federal health care reform initiatives of the early- to mid-1990s were inspired in part by public concern about the privacy of personal medical information as the use of health IT increased. Congress, recognizing that benefits and efficiencies could be gained by the use of information technology in health care, also recognized the need for comprehensive federal medical privacy protections and consequently passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This law provided for the Secretary of HHS to establish the first broadly applicable federal privacy and security protections designed to protect individual health care information.

HIPAA required the Secretary of HHS to promulgate regulatory standards to protect certain personal health information held by covered entities, which are certain health plans, health care

[9]GAO, *Health Information Technology: HHS Is Taking Steps to Develop a National Strategy*, GAO-05-628 (Washington, D.C.: May 27, 2005); GAO, *Health Information Technology: HHS Is Continuing Efforts to Define a National Strategy*, GAO-06-346T (Washington, D.C.: Mar. 15, 2006); GAO-06-1071T.

providers, and health care clearinghouses.[10] It also required the Secretary of HHS to adopt security standards for covered entities that maintain or transmit health information to maintain reasonable and appropriate safeguards. The law requires that covered entities take certain measures to ensure the confidentiality and integrity of the information and to protect it against reasonably anticipated unauthorized use or disclosure and threats or hazards to its security.

HIPAA provides authority to the Secretary to enforce these standards. The Secretary has delegated administration and enforcement of privacy standards to the department's Office for Civil Rights and enforcement of the security standards to the department's Centers for Medicare and Medicaid Services.

Most states have statutes that in varying degrees protect the privacy of personal health information. HIPAA recognizes this and specifically provides that its implementing regulations do not preempt contrary provisions of state law if the state laws impose more stringent requirements, standards, or specifications than the federal privacy rule. In this way, the law and its implementing rules establish a baseline of mandatory minimum privacy protections and define basic principles for protecting personal health information.

The Secretary of HHS first issued HIPAA's Privacy Rule in December 2000, following public notice and comment, but later modified the rule in August 2002. Subsequent to the issuance of the Privacy Rule, the Secretary issued the Security Rule in February 2003 to safeguard electronic protected health information and help ensure that covered entities have proper security controls in place

[10]HIPAA's protection of health information is limited by the scope of its defined terms. "Health information" is defined as any information that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse and related to any physical or mental health or condition of an individual, the provision of health care to an individual, or any payment for the provision of health care to an individual. "Covered entities" are health plans that provide or pay for the medical care of individuals, health care providers that electronically transmit health information in connection with any of the transactions regulated by the statute, and health care clearinghouses that receive health information from other entities and process or facilitate the processing of that information for those entities. Our description of HIPAA's protection of the privacy or personal health information is limited accordingly.

to provide assurance that the information is protected from unwarranted or unintentional disclosure.

The Privacy Rule reflects basic privacy principles for ensuring the protection of personal health information. Table 1 summarizes these principles.

Table 1: Key Privacy Principles in HIPAA's Privacy Rule

HIPAA Privacy Rule principle	
Uses and disclosures	Provides limits to the circumstances in which an individual's protected health information may be used or disclosed by covered entities and provides for accounting of certain disclosures; requires covered entities to make reasonable efforts to disclose or use only the minimum information necessary to accomplish the intended purpose for the uses, disclosures, or requests, with certain exceptions such as for treatment or as required by law.
Notice	Requires most covered entities to provide a notice of their privacy practices including how personal health information may be used and disclosed.
Access	Establishes individuals' rights to review and obtain a copy of their protected health information held in a designated record set.[a]
Security[b]	Requires covered entities to safeguard protected health information from inappropriate use or disclosure.
Amendments	Gives individuals the right to request from covered entities changes to inaccurate or incomplete protected health information held in a designated record set.[a]
Administrative requirements	Requires covered entities to analyze their own needs and implement solutions appropriate for their own environment based on a basic set of requirements for which they are accountable.
Authorization	Requires covered entities to obtain the individual's written authorization for uses and disclosures of personal health information with certain exceptions, such as for treatment, payment, and health care operations, or as required by law. Covered entities may choose to obtain the individual's consent to use or disclose protected health information to carry out treatment, payment, or health care operations, but are not required to do so.

Source: GAO analysis of HIPAA Privacy Rule.

[a] According to the Privacy Rule, a designated record set is a group of records maintained by or for a covered entity that are (1) the medical records and billing records about individuals maintained by or for a covered health care provider; (2) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (3) used, in whole or in part, by or for the covered entity to make decisions about individuals.

[b] The Security Rule further defines safeguards that covered entities must implement to provide assurance that health information is protected from inappropriate use and disclosure.

HHS Has Initiated Actions to Identify Solutions for Protecting Personal Health Information but Has Not Defined an Overall Approach for Addressing Privacy

HHS and its Office of the National Coordinator for Health IT have initiated actions to identify solutions for protecting health information. Specifically, HHS awarded several health IT contracts that include requirements for developing solutions that comply with federal privacy and security requirements, consulted with the National Committee on Vital and Health Statistics (NCVHS) to develop recommendations regarding privacy and confidentiality in the Nationwide Health Information Network, and formed the American Health Information Community (AHIC) Confidentiality, Privacy, and Security Workgroup to frame privacy and security policy issues and identify viable options or processes to address these issues. The Office of the National Coordinator for Health IT intends to use the results of these activities to identify technology and policy solutions for protecting personal health information as part of its continuing efforts to complete a national strategy to guide the nationwide implementation of health IT. However, HHS is in the early stages of identifying solutions for protecting personal health information and has not yet defined an overall approach for integrating its various privacy-related initiatives and for addressing key privacy principles.

HHS's Contracts Are to Address Privacy and Security Policy and Standards for Nationwide Health Information Exchange

HHS awarded four major health IT contracts in 2005 intended to advance the nationwide exchange of health information—Privacy and Security Solutions for Interoperable Health Information Exchange, Standards Harmonization Process for Health IT, Nationwide Health Information Network Prototypes, and Compliance Certification Process for Health IT. These contracts include requirements for developing solutions that comply with federal privacy requirements. The contract for privacy and security solutions is intended to specifically address privacy and security policies and practices that affect nationwide health information exchange.

HHS's contract for privacy and security solutions is intended to provide a nationwide synthesis of information to inform privacy and security policymaking at federal, state, and local levels and the Nationwide Health Information Network prototype solutions for supporting health information exchange across the nation. In summer 2006, the privacy and security solutions contractor selected 34 states and territories as locations in which to perform assessments of organization-level privacy- and security-related policies and practices that affect interoperable electronic health information exchange and their bases, including laws and regulations. The contractor is supporting the states and territories as they (1) assess variations in organization-level business policies and state laws that affect health information exchange, (2) identify and propose solutions while preserving the privacy and security requirements of applicable federal and state laws, and (3) develop detailed plans to implement solutions.

The privacy and security solutions contractor is to develop a nationwide report that synthesizes and summarizes the variations identified, the proposed solutions, and the steps that states and territories are taking to implement their solutions. It is also to deliver an interim report to address policies and practices followed in nine domains of interest: (1) user and entity authentication, (2) authorization and access controls, (3) patient and provider identification to match identities, (4) information transmission security or exchange protocols (encryption, etc.), (5) information protections to prevent improper modification of records, (6) information audits that record and monitor the activity of health information systems, (7) administrative or physical security safeguards required to implement a comprehensive security platform for health IT, (8) state law restrictions about information types and classes and the solutions by which electronic personal health information can be viewed and exchanged, and (9) information use and disclosure policies that arise as health care entities share clinical health information electronically. These domains of interest address the use and disclosure and security privacy principles.

The National Committee on Vital and Health Statistics Made Recommendations for Addressing Privacy and Security within a Nationwide Health Information Network

In June 2006, NCVHS, a key national health information advisory committee, presented to the Secretary of HHS a report recommending actions regarding privacy and confidentiality in the Nationwide Health Information Network. The recommendations cover topics that are, according to the committee, central to challenges for protecting health information privacy in a national health information exchange environment. The recommendations address aspects of key privacy principles including (1) the role of individuals in making decisions about the use of their personal health information, (2) policies for controlling disclosures across a nationwide health information network, (3) regulatory issues such as jurisdiction and enforcement, (4) use of information by non-health care entities, and (5) establishing and maintaining the public trust that is needed to ensure the success of a nationwide health information network. The recommendations are being evaluated by the AHIC work groups, the Certification Commission for Health IT, the Health Information Technology Standards Panel, and other HHS partners.

In October 2006, the committee recommended that HIPAA privacy protections be extended beyond the current definition of covered entities to include other entities that handle personal health information. It also called on HHS to create policies and procedures to accurately match patients with their health records and to require functionality that allows patient or physician privacy preferences to follow records regardless of location. The committee intends to continue to update and refine its recommendations as the architecture and requirements of the network advance.

The American Health Information Community's Confidentiality, Privacy, and Security Workgroup Is to Develop Recommendations to Establish a Privacy Policy Framework

AHIC, a commission that provides input and recommendations to HHS on nationwide health IT, formed the Confidentiality, Privacy, and Security Workgroup in July 2006 to frame privacy and security

policy issues and to solicit broad public input to identify viable options or processes to address these issues.[11] The recommendations to be developed by this work group are intended to establish an initial policy framework and address issues including methods of patient identification, methods of authentication, mechanisms to ensure data integrity, methods for controlling access to personal health information, policies for breaches of personal health information confidentiality, guidelines and processes to determine appropriate secondary uses of data, and a scope of work for a long-term independent advisory body on privacy and security policies.

The work group has defined two initial work areas—identity proofing[12] and user authentication[13]—as initial steps necessary to protect confidentiality and security. These two work areas address the security principle. Last month, the work group presented recommendations on performing patient identity proofing to AHIC. The work group intends to address other key privacy principles, including, but not limited to maintaining data integrity and control of access. It plans to address policies for breaches of confidentiality and guidelines and processes for determining appropriate secondary uses of health information, an aspect of the use and disclosure privacy principle.

[11]In May 2006, several of the AHIC work groups recommended the formation of an additional work group composed of privacy, security, clinical, and technology experts from each of the other AHIC work groups. The AHIC Confidentiality, Privacy, and Security Workgroup first convened in August 2006.

[12]Identity proofing is the process of providing sufficient information (e.g., identity history, credentials, documents) to establish and verify a person's identity. Identity proofing already takes place throughout many industries, including health care. However, a standard methodology does not exist.

[13]User authentication is the process of confirming a person's claimed identity, often used as a way to grant access to data, resources, and other network services. While a user name and password provide a foundational level of authentication, several other techniques, most notably two-factor authentication, have additional capabilities.

HHS's Collective Initiatives Are Intended to Address Aspects of Key Privacy Principles, but an Overall Approach for Addressing Privacy Has Not Been Defined

HHS has taken steps intended to address aspects of key privacy principles through its contracts and with advice and recommendations from its two key health IT advisory committees. For example, the privacy and security solutions contract is intended to address all the key privacy principles in HIPAA. Additionally, the uses and disclosures principle is to be further addressed through the advisory committees' recommendations and guidance. The security principle is to be addressed through the definition of functional requirements for a nationwide health information network, the definition of security criteria for certifying electronic health record products, the identification of information exchange standards, and recommendations from the advisory committees regarding, among other things, methods to establish and confirm a person's identity. The committees have also made recommendations for addressing authorization for uses and disclosure of health information and intend to develop guidelines for determining appropriate secondary uses of data.

HHS has made some progress toward protecting personal health information through its various privacy-related initiatives. For example, during the past 2 years, HHS has defined initial criteria and procedures for certifying electronic health records, resulting in the certification of 35 IT vendor products. In January 2007, HHS contractors presented 4 initial prototypes of a Nationwide Health Information Network (NHIN). However, the other contracts have not yet produced final results. For example, the privacy and security solutions contractor has not yet reported its assessment of state and organizational policy variations. This report is due on March 31, 2007. Additionally, HHS has not accepted or agreed to implement the recommendations made in June 2006 by the NCVHS, and the AHIC Privacy, Security, and Confidentiality Workgroup is in the very early stages of efforts that are intended to result in privacy policies for nationwide health information exchange.

HHS is in the early phases of identifying solutions for safeguarding personal health information exchanged through a nationwide health information network and has not yet defined an approach for

integrating its various efforts or for fully addressing key privacy principles. For example, milestones for integrating the results of its various privacy-related initiatives and resolving differences and inconsistencies have not been defined, and it has not been determined which entity participating in HHS's privacy-related activities is responsible for integrating these various initiatives and the extent to which their results will address key privacy principles. Until HHS defines an integration approach and milestones for completing these steps, its overall approach for ensuring the privacy and protection of personal health information exchanged throughout a nationwide network will remain unclear.

The Health Care Industry Faces Challenges in Protecting Electronic Health Information

The increased use of information technology to exchange electronic health information introduces challenges to protecting individuals' personal health information. In our report, we identify and summarize key challenges described by health information exchange organizations: understanding and resolving legal and policy issues, particularly those resulting from varying state laws and policies; ensuring appropriate disclosures of the minimum amount of health information needed; ensuring individuals' rights to request access to and amendments of health information to ensure it is correct; and implementing adequate security measures for protecting health information. Table 2 summarizes these challenges.

Table 2: Challenges to Exchanging Electronic Health Information

Area	
Understanding and resolving legal and policy issues	• Resolving uncertainties regarding varying the extent of federal privacy protection required of various organizations • Understanding and resolving data-sharing issues introduced by varying state privacy laws and organization-level practices • Reaching agreement on organizations' differing interpretations and applications of HIPAA privacy and security rules • Determining liability and enforcing sanctions in cases of breach of confidentiality
Ensuring appropriate disclosure	• Determining the minimum data necessary that can be disclosed in order for requesters to accomplish their intended purposes • Obtaining individuals' authorization and consent for use and disclosure of personal health information • Determining the best way to allow individuals to participate in and consent to electronic health information exchange • Educating consumers so that they understand the extent to which their consent to use and disclose health information applies
Ensuring individuals' rights to request access and amendments to health information to ensure it is correct	• Ensuring that individuals understand that they have rights to request access and amendments to their own health information to ensure that it is correct • Ensuring that individuals' amendments are properly made and tracked across multiple locations
Implementing adequate security measures for protecting health information	• Determining and implementing adequate techniques for authenticating requesters of health information • Implementing proper access controls and maintaining adequate audit trails for monitoring access to health data • Protecting data stored on portable devices and transmitted between business partners

Source: GAO analysis of information provided by state-level health information exchange organizations, federal health care providers, and health IT professional associations.

Understanding and Resolving Legal and Policy Issues

Health information exchange organizations bring together multiple and diverse health care providers, including physicians, pharmacies, hospitals, and clinics that may be subject to varying legal and policy requirements for protecting health information. As health information exchange expands across state lines, organizations are challenged with understanding and resolving data-sharing issues introduced by varying state privacy laws. HHS recognized that sharing health information among entities in states with varying laws introduces challenges and intends to identify variations in state laws that affect privacy and security practices through the privacy and security solutions contract that it awarded in 2005.

Ensuring Appropriate Disclosure

Several organizations described issues associated with ensuring appropriate disclosure, such as determining the minimum data necessary that can be disclosed in order for requesters to accomplish the intended purposes for the use of the health information. For example, dieticians and health claims processors do not need access to complete health records, whereas treating physicians generally do. Organizations also described issues with obtaining individuals' authorization and consent for uses and disclosures of personal health information and difficulties with determining the best way to allow individuals to participate in and consent to electronic health information exchange. In June 2006, NCVHS recommended to the Secretary of HHS that the department monitor the development of different approaches and continue an open, transparent, and public process to evaluate whether a national policy on this issue would be appropriate.

Ensuring Individuals' Rights to Request Access and Amendments to Health Information to Ensure It Is Correct

As the exchange of personal health information expands to include multiple providers and as individuals' health records include increasing amounts of information from many sources, keeping track of the origin of specific data and ensuring that incorrect information is corrected and removed from future health information exchange could become increasingly difficult. Additionally, as health information is amended, HIPAA rules require that covered entities make reasonable efforts to notify certain providers and other persons that previously received the individuals' information. The challenges associated with meeting this requirement are expected to become more prevalent as the numbers of organizations exchanging health information increases.

Implementing Adequate Security Measures for Protecting Health Information

Adequate implementation of security measures is another challenge that health information exchange providers must overcome to ensure that health information is adequately protected as health information exchange expands. For example, user authentication

will become more difficult when multiple organizations that employ different techniques exchange information. The AHIC Confidentiality, Privacy, and Security Workgroup recognized this difficulty and identified user authentication as one of its initial work areas for protecting confidentiality and security.

Implementation of GAO Recommendations Should Help Ensure that HHS'S Goal to Protect Personal Health Information is Met

To increase the likelihood that HHS will meet its strategic goal to protect personal health information, we recommend in our report[14] that the Secretary of Health and Human Services define and implement an overall approach for protecting health information as part of the strategic plan called for by the President. This approach should:

1. Identify milestones and the entity responsible for integrating the outcomes of its privacy-related initiatives, including the results of its four health IT contracts and recommendations from the NCVHS and AHIC advisory committees.
2. Ensure that key privacy principles in HIPAA are fully addressed.
3. Address key challenges associated with legal and policy issues, disclosure of personal health information, individuals' rights to request access and amendments to health information, and security measures for protecting health information within a nationwide exchange of health information.

In commenting on a draft of our report, HHS disagreed with our recommendation and referred to "the department's comprehensive and integrated approach for ensuring the privacy and security of health information within nationwide health information exchange." However, an overall approach for integrating the department's various privacy-related initiatives has not been fully defined and

[14]GAO-07-238.

implemented. While progress has been made initiating these efforts, much work remains before they are completed and the outcomes of the various efforts are integrated. HHS specifically disagreed with the need to identify milestones and stated that tightly scripted milestones would impede HHS's processes and preclude stakeholder dialogue on the direction of important policy matters. We disagree and believe that milestones are important for setting targets for implementation and for informing stakeholders of HHS's plans and goals for protecting personal health information as part of its efforts to achieve nationwide implementation of health IT.

HHS did not comment on the need to identify an entity responsible for the integration of the department's privacy-related initiatives, nor did it provide information regarding an effort to assign responsibility for this important activity. HHS neither agreed nor disagreed that its approach should address privacy principles and challenges, but stated that the department plans to continue to work toward addressing privacy principles in HIPAA and that our report appropriately highlights efforts to address challenges encountered during electronic health information exchange. HHS stated that the department is committed to ensuring that health information is protected as part of its efforts to achieve nationwide health information exchange.

In written comments, the Secretary of Veterans Affairs concurred with our findings, conclusions, and recommendation to the Secretary of HHS and commended our efforts to highlight methods for ensuring the privacy of electronic health information. The Department of Defense chose not to comment on a draft of the report.

In summary, concerns about the protection of personal health information exchanged electronically within a nationwide health information network have increased as the use of health IT and the exchange of electronic health information have also increased. HHS and its Office of the National Coordinator for Health IT have initiated activities that, collectively, are intended to protect health information and address aspects of key privacy principles. While

progress continues to be made through the various initiatives, it becomes increasingly important that HHS define a comprehensive approach and milestones for integrating its efforts, resolve differences and inconsistencies among them, fully address key privacy principles, ensure that recommendations from its advisory committees are effectively implemented, and sequence the implementation of key activities appropriately.

HHS's current initiatives are intended to address many of the challenges that organizations face as the exchange of electronic health information expands. However, without a clearly defined approach that establishes milestones for integrating efforts and fully addresses key privacy principles and the related challenges, it is likely that HHS's goal to safeguard personal health information as part of its national strategy for health IT will not be met.

Mr. Chairman, Senator Voinovich, and members of the subcommittee, this concludes our statement. We will be happy to answer any questions that you or members of the subcommittee may have at this time.

Contacts and Acknowledgments

If you have any questions on matters discussed in this testimony, please contact Linda Koontz at (202) 512-6240 or David Powner at (202) 512-9286, or by e-mail at koontzl@gao.gov or pownerd@gao.gov. Other key contributors to this testimony include Mirko J. Dolak, Amanda C. Gill, Nancy E. Glover, M. Saad Khan, David F. Plocher, Charles F. Roney, Sylvia L. Shanks, Sushmita L. Srikanth, Teresa F. Tucker, and Morgan F. Walts.

United States Government Accountability Office

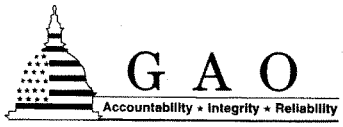
GAO

Report to Congressional Requesters

January 2007

HEALTH INFORMATION TECHNOLOGY

Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy



GAO-07-238

Abbreviations

AHIC	American Health Information Community
DOD	Department of Defense
Health IT	health information technology
HIPAA	Health Insurance Portability and Accountability Act of 1996
HHS	Health and Human Services
NCVHS	National Committee on Vital and Health Statistics
NHIN	Nationwide Health Information Network
VA	Department of Veterans Affairs

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

January 2007

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-238, a report to congressional requesters

HEALTH INFORMATION TECHNOLOGY

Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy

Why GAO Did This Study

The expanding implementation of health information technology (IT) and electronic health information exchange networks raises concerns regarding the extent to which the privacy of individuals' electronic health information is protected. In April 2004, President Bush called for the Department of Health and Human Services (HHS) to develop and implement a strategic plan to guide the nationwide implementation of health IT. The plan is to recommend methods to ensure the privacy of electronic health information.

GAO was asked to describe HHS's efforts to ensure privacy as part of its national strategy and to identify challenges associated with protecting electronic personal health information. To do this, GAO assessed relevant HHS privacy-related initiatives and analyzed information from health information organizations.

What GAO Recommends

GAO recommends that HHS define and implement an overall privacy approach that identifies milestones for integrating the outcomes of its initiatives, ensures that key privacy principles are fully addressed, and addresses challenges associated with the nationwide exchange of health information. In its comments, HHS disagreed and stated that it has established a comprehensive privacy approach. However, GAO believes that an overall approach for integrating HHS's initiatives has not been fully defined and implemented.

www.gao.gov/cgi-bin/getrpt?GAO-07-238.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Linda D. Koontz, (202) 512-6240 or koontzl@gao.gov.

What GAO Found

HHS and its Office of the National Coordinator for Health IT have initiated actions to identify solutions for protecting personal health information through several contracts and with two health information advisory committees. For example, in late 2005, HHS awarded several health IT contracts that include requirements for addressing the privacy of personal health information exchanged within a nationwide health information exchange network. Its privacy and security solutions contractor is to assess the organization-level privacy- and security-related policies, practices, laws, and regulations that affect interoperable health information exchange. Additionally, in June 2006, the National Committee on Vital and Health Statistics made recommendations to the Secretary of HHS on protecting the privacy of personal health information within a nationwide health information network, and in August 2006, the American Health Information Community convened a work group to address privacy and security policy issues for nationwide health information exchange. While these activities are intended to address aspects of key principles for protecting the privacy of health information, HHS is in the early stages of its efforts and has therefore not yet defined an overall approach for integrating its various privacy-related initiatives and addressing key privacy principles, nor has it defined milestones for integrating the results of these activities.

GAO identified key challenges associated with protecting electronic personal health information in four areas (see table).

Challenges to Exchanging Electronic Health Information

Area	
Understanding and resolving legal and policy issues	• Resolving uncertainties regarding the extent of federal privacy protection required of various organizations • Understanding and resolving data sharing issues introduced by varying state privacy laws and organization-level practices • Reaching agreements on differing interpretations and applications of HIPAA privacy and security rules • Determining liability and enforcing sanctions in case of breaches of confidentiality
Ensuring appropriate disclosure	• Determining the minimum data necessary that can be disclosed in order for requesters to accomplish their intended purposes • Determining the best way to allow patients to participate in and consent to electronic health information exchange • Educating consumers about the extent to which their consent to use and disclose health information applies
Ensuring individuals' rights to request access and amendments to health information	• Ensuring that individuals understand that they have rights to access and amend their own health information • Ensuring that individuals' amendments are properly made and tracked across multiple locations
Implementing adequate security measures for protecting health information	• Determining and implementing adequate techniques for authenticating requesters of health information • Implementing proper access controls and maintaining adequate audit trails for monitoring access to health data • Protecting data stored on portable devices and transmitted between business partners

Source: GAO analysis of information provided by state-level health information exchange organizations, federal health care providers, and health IT professional associations.

Contents

Letter

Results in Brief	1
Background	3
HHS Has Initiated Actions to Identify Solutions for Protecting Personal Health Information but Has Not Defined an Overall Approach for Addressing Privacy	6
The Health Care Industry Faces Challenges in Protecting Electronic Health Information	14
Conclusions	21
Recommendation for Executive Action	27
Agency Comments and Our Evaluation	28
	28

Appendixes

Appendix I:	**Objectives, Scope, and Methodology**	32
Appendix II:	**Major Federal Health Care Programs**	35
Appendix III:	**HHS Health IT Contracts**	36
Appendix IV:	**The Office of the National Coordinator for Health IT's Goals, Objectives, and Strategies**	39
Appendix V:	**Descriptions of Federal Laws for Protecting Personal Health Information**	41
Appendix VI:	**Comments from the Department of Health and Human Services**	44
Appendix VII:	**Comments from the Department of Veterans Affairs**	51
Appendix VIII:	**GAO Contacts and Acknowledgments**	52

Tables

Table 1:	Key Privacy Principles in HIPAA's Privacy Rule	13
Table 2:	Key HIPAA Privacy Principles and HHS's Initiatives Intended to Address Aspects of the Principles	19
Table 3:	Challenges to Exchanging Electronic Health Information	22
Table 4:	Federal Programs	35
Table 5:	HHS Health IT Contracts	36
Table 6:	Goals, Objectives, and Strategies of the Office of the National Coordinator	39
Table 7:	Selected Federal Laws that Protect Personal Health Information	41

United States Government Accountability Office
Washington, D.C. 20548

January 10, 2007

The Honorable Daniel K. Akaka
Chairman
Subcommittee on Oversight of Government
Management, the Federal Workforce,
and the District of Columbia
Committee on Homeland Security
and Governmental Affairs
U.S. Senate

The Honorable Edward M. Kennedy
Chairman
Committee on Health, Education, Labor
and Pensions
U.S. Senate

The expanding implementation of health information technology (health IT)[1] and electronic health care information exchange networks raises concerns regarding the extent to which individuals' privacy is protected. Inappropriate disclosure of personal health information[2] could result in information being revealed that individuals wish to keep confidential. Recent incidents in which unauthorized persons accessed data and where employees' laptops containing personal information were stolen highlight the vulnerability of electronic personal information and the reservations the public has about sharing personal health information electronically.

Key privacy principles for protecting personal information have been in existence for years and provide a foundation for privacy laws, practices, and policies. Those privacy principles are reflected in the provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which define the circumstances under which an individual's health information may be used or disclosed. In addition, HIPAA's security

[1]Health IT is the use of technology to electronically collect, store, retrieve, and transfer clinical, administrative, and financial health information. Health IT is interoperable when systems are able to exchange data accurately, effectively, securely, and consistently with different IT systems, software applications, and networks in such a way that the clinical or operational purposes and meaning of the data are preserved and unaltered.

[2]Use of the term "personal health information" throughout this report refers to information relating to the health or health care of an individual that identifies, or can be used to identify, the individual.

provisions require entities that hold or transmit personal health information to maintain reasonable safeguards to protect it against unauthorized use or disclosure and ensure its integrity and confidentiality. In April 2004, President Bush issued an executive order that called for the development and implementation of a strategic plan to guide the nationwide implementation of interoperable health IT in both the public and private sectors.[3] The plan is to address privacy and security issues related to interoperable health IT and recommend methods to ensure appropriate authorization, authentication, and encryption of data for transmission over the Internet. The order established the position of the National Coordinator for Health Information Technology within the Department of Health and Human Services (HHS) as the government official responsible for developing and implementing a strategic plan for health IT.

You asked us to describe HHS's efforts to help ensure the privacy of health information. Specifically, our objectives were to

- describe the steps HHS is taking to ensure privacy protection as part of the national health IT strategy and
- identify challenges associated with meeting requirements for protecting personal health information within a nationwide health information network.

To address our first objective, we focused our analytical work on HHS because it is responsible for development and implementation of a national health information technology strategy that is to include the protection of personal health information. We evaluated information from and held discussions with officials from HHS components and advisory committees that play major roles in supporting HHS's efforts to ensure the protection of electronic health information exchanged within a nationwide health information network.

To address the second objective, we reviewed and analyzed information obtained from documentation provided by and discussions held with officials from federal agencies that provide health care services—the

[3]Executive Order 13335, *Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator* (Washington, D.C.: Apr. 27, 2004).

Centers for Medicare and Medicaid Services, the Departments of Defense and Veterans Affairs, and the Indian Health Service—and representatives from selected state-level health information exchange organizations. We selected organizations that are currently exchanging electronic health information to obtain examples of challenges they face in protecting health information as they implement electronic health information exchange systems. We analyzed the information they provided to identify key challenges faced throughout the health care industry as the implementation of electronic health information exchange expands. Further details about our objectives, scope, and methodology are provided in appendix I. We performed our work from December 2005 through November 2006 in accordance with generally accepted government auditing standards.

Results in Brief

HHS and its Office of the National Coordinator for Health IT have initiated actions to study the protection of personal health information through the work of several contracts, the National Committee on Vital and Health Statistics,[4] and the American Health Information Community.[5] For example:

- In late 2005, HHS awarded several health IT contracts that include requirements for addressing the privacy of personal health information exchanged within an electronic nationwide health information network.
- In summer 2006, HHS's contractor for privacy and security solutions selected 33 states and Puerto Rico as locations in which to perform assessments of organization-level privacy- and security-related policies, practices, laws, and regulations that affect interoperable health information exchange and to propose privacy and security protections that permit interoperability.

[4]The National Committee on Vital and Health Statistics was established in 1949 as a public advisory committee that is statutorily authorized to advise the Secretary of HHS on health data, statistics, and national health information policy, including the implementation of health IT standards.

[5]The American Health Information Community is a federally chartered advisory committee made up of representatives from both the public and private health care sectors. The community provides input and recommendations to HHS on making health records electronic and providing assurance that the privacy and security of those records are protected.

- In June 2006, the National Committee on Vital and Health Statistics provided a report to the Secretary of HHS that made recommendations on protecting the privacy of personal health information within a nationwide health information network.

- In August 2006, the American Health Information Community also convened a work group to address privacy and security policy issues for nationwide health information exchange.

HHS and its Office of the National Coordinator for Health IT intend to use the results of these activities to identify technology and policy solutions for protecting personal health information as part of their continuing efforts to complete a national strategy to guide the nationwide implementation of health IT. While these activities are intended to address aspects of key principles for protecting health information, HHS is in the early stages of its efforts and has therefore not yet defined an overall approach for integrating its various privacy-related initiatives and addressing key privacy principles. In addition, milestones for integrating the results of these activities do not yet exist. Until HHS defines an integration approach and milestones for completing these steps, its overall approach for ensuring the privacy and protection of personal health information exchanged throughout a nationwide network will remain unclear.

Key challenges associated with protecting personal health information are understanding and resolving legal and policy issues, such as those related to variations in states' privacy laws; ensuring that only the minimum amount of information necessary is disclosed to only those entities authorized to receive the information; ensuring individuals' rights to request access and amendments to their own health information; and implementing adequate security measures for protecting health information.

We are recommending that the Secretary of HHS define and implement an overall approach for protecting health information as part of the strategic plan called for by the President. This approach should (1) identify milestones for integrating the outcomes of HHS's privacy-related initiatives, (2) ensure that key privacy principles are fully addressed, and (3) address key challenges associated with the nationwide exchange of health information.

We received written comments on a draft of this report from HHS's Assistant Secretary for Legislation. The Assistant Secretary disagreed with

our recommendation. Throughout the comments, the Assistant Secretary referred to the department's comprehensive and integrated approach for ensuring the privacy and security of health information within nationwide health information exchange. However, an overall approach for integrating the department's various privacy-related initiatives has not been fully defined and implemented. We acknowledge in our report that HHS has established a strategic objective to protect consumer privacy along with two specific strategies for meeting this objective. Our report also acknowledges the key efforts that HHS has initiated to address this objective, and HHS's comments describe these and additional state and federal efforts. HHS stated that the department has made significant progress in integrating these efforts. While progress has been made initiating these efforts, much work remains before they are completed and the outcomes of the various efforts are integrated. Thus, we recommended that HHS define and implement a comprehensive privacy approach that includes milestones for integration, identifies the entity responsible for integrating the outcomes of its privacy-related initiatives, addresses key privacy principles, and ensures that challenges are addressed in order to meet the department's objective to protect the privacy of health information exchanged within a nationwide health information network.

HHS specifically disagreed with the need to identify milestones and stated that tightly scripted milestones would impede HHS's processes and preclude stakeholder dialogue on the direction of important policy matters. We disagree and believe that milestones are important for setting targets for implementation and informing stakeholders of HHS's plans and goals for protecting personal health information as part of its efforts to achieve nationwide implementation of health IT. Milestones are especially important considering the need for HHS to integrate and coordinate the many deliverables of its numerous ongoing and remaining activities. We agree that it is important for HHS to continue to actively involve both public and private sector health care stakeholders in its processes. HHS did not comment on the need to identify an entity responsible for the integration of the department's privacy-related initiatives, nor did it provide information regarding any effort to assign responsibility for this important activity. HHS neither agreed nor disagreed that its approach should address privacy principles and challenges, but stated that the department plans to continue to work toward addressing privacy principles in HIPAA and that our report appropriately highlights efforts to address challenges encountered during electronic health information exchange.

In his written comments, The Secretary of Veterans Affairs (VA) concurred with our findings, conclusions, and recommendations to the Secretary of HHS and commended our efforts to highlight methods for ensuring the privacy of electronic health information. Both agencies provided technical comments, which we have incorporated into the report as appropriate.

Written comments from HHS and VA are reproduced in appendixes VI and VII. The Department of Defense (DOD) chose not to comment on a draft of this report.

Background

Studies published by the Institute of Medicine and other organizations have indicated that fragmented, disorganized, and inaccessible clinical information adversely affects the quality of health care and compromises patient safety. In addition, long-standing problems with medical errors and inefficiencies increase costs for health care delivery in the United States. With health care spending in 2004 reaching almost $1.9 trillion, or 16 percent, of the gross domestic product, concerns about the costs of health care continue. As we reported last year, many policy makers, industry experts, and medical practitioners contend that the U.S. health care system is in a crisis.[6]

Health IT provides a promising solution to help improve patient safety and reduce inefficiencies. The expanded use of health IT has great potential to improve the quality of care, bolster the preparedness of our public health infrastructure, and save money on administrative costs. As we reported in 2003, technologies such as electronic health records and bar coding of certain human drug and biological product labels have been shown to save money and reduce medical errors.[7] Health care organizations reported that IT contributed other benefits, such as shorter hospital stays, faster communication of test results, improved management of chronic diseases, and improved accuracy in capturing charges associated with diagnostic and procedure codes. Over the past several years, a growing number of communities have established health information exchange organizations that allow multiple health care providers, such as physicians, clinical

[6]GAO, *21st Century Challenges: Reexamining the Base of the Federal Government*, GAO-05-325SP (Washington, D.C.: February 2005).

[7]GAO, *Information Technology: Benefits Realized for Selected Health Care Functions*, GAO-04-224 (Washington, D.C.: Oct. 31, 2003).

laboratories, and emergency rooms to share patients' electronic health information. Most of these organizations are in either the planning or early implementation phases of establishing electronic health information exchange.

Federal Government's Role in Health Care

According to the Institute of Medicine, the federal government has a central role in shaping nearly all aspects of the health care industry as a regulator, purchaser, health care provider, and sponsor of research, education, and training. Seven major federal health care programs, such as the Centers for Medicare and Medicaid Services (CMS), DOD's TRICARE, VA's Veterans Health Administration, and HHS's Indian Health Service, provide or fund health care services to approximately 115 million Americans. According to HHS, federal agencies fund more than a third of the nation's total health care costs. Given the level of the federal government's participation in providing health care, it has been urged to take a leadership role in driving change to improve the quality and effectiveness of medical care in the United States, including expanded adoption of IT. The programs and number of citizens who receive health care services from the federal government and the cost of these services are summarized in appendix II.

In April 2004, President Bush called for the widespread adoption of interoperable electronic health records within 10 years and issued an executive order that established the position of the National Coordinator for Health Information Technology within HHS as the government official responsible for the development and execution of a strategic plan to guide the nationwide implementation of interoperable health IT in both the public and private sectors.[8] In July 2004, HHS released *The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care—Framework for Strategic Action*.[9] This framework described goals for achieving nationwide interoperability of health IT and actions to be taken by both the public and private sectors in implementing a strategy. HHS's Office of the National Coordinator for Health IT updated the framework's goals in June 2006 and included an

[8]Executive Order 13335.

[9]Department of Health and Human Services, *"The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care: A Framework for Strategic Action"* (Washington, D.C.: July 21, 2004).

objective for protecting consumer privacy. It identified two specific strategies for meeting this objective—(1) support the development and implementation of appropriate privacy and security policies, practices, and standards for electronic health information exchange and (2) develop and support policies to protect against discrimination based on personal health information such as denial of medical insurance or employment.

Need for a National Strategy and Adoption of Interoperable Health IT

In July 2004, we testified on the benefits that effective implementation of IT can bring to the health care industry and the need for HHS to provide continued leadership, clear direction, and mechanisms to monitor progress in order to bring about measurable improvements.[10] Since then, we have reported or testified on several occasions on HHS's efforts to define its national strategy for health IT. We recommended that HHS develop the detailed plans and milestones needed to ensure that its goals are met, and HHS agreed with our recommendation.[11]

In our report and testimonies, we have described a number of actions that HHS, through the Office of the National Coordinator for Health IT, has taken toward accelerating the use of IT to transform the health care industry,[12] including the development of the framework for strategic action. We described the formation of a public-private advisory body—the American Health Information Community—to advise HHS on achieving interoperability for health information exchange and four breakthrough areas[13] the community identified—consumer empowerment, chronic care, biosurveillance, and electronic health records. Additionally, we reported that, in late 2005, HHS's Office of the National Coordinator for Health IT awarded $42 million in contracts to address a range of issues important for developing a robust health IT infrastructure. In October 2006, HHS's Office

[10]GAO, *Health Care: National Strategy Needed to Accelerate the Implementation of Information Technology*, GAO-04-947T (Washington, D.C.: July 14, 2004).

[11]GAO, *Health Information Technology: HHS Is Continuing Efforts to Define Its National Strategy*, GAO-06-1071T (Washington, D.C.: Sept. 1, 2006).

[12]GAO, *Health Information Technology: HHS Is Taking Steps to Develop a National Strategy*, GAO-05-628 (Washington, D.C.: May 27, 2005); GAO, *Health Information Technology: HHS Is Continuing Efforts to Define a National Strategy*, GAO-06-346T (Washington, D.C.: Mar. 15, 2006); GAO-06-1071T.

[13]Breakthrough areas are components of health care and public health that can potentially achieve measurable results in 2 to 3 years.

of the National Coordinator for Health IT awarded an additional contract to form a state-level electronic health alliance and address challenges to health information exchange, including privacy and security issues. HHS intends to use the results of the contracts and recommendations from the National Committee on Vital and Health Statistics and the American Health Information Community proceedings to define the future direction of a national strategy. The contracts are described in appendix III.

We have also described the Office of the National Coordinator's continuing efforts to work with other federal agencies to revise and refine the goals and strategies identified in its initial framework. The current draft framework—*The Office of the National Coordinator: Goals, Objectives, and Strategies*—identifies objectives for accomplishing each of four goals, along with 32 high-level strategies for meeting the objectives. It includes a specific objective for safeguarding consumer privacy and protecting against risks along with two strategies for meeting this objective: (1) support the development and implementation of appropriate privacy and security policies, practices, and standards for electronic health information exchange and (2) develop and support policies to protect against discrimination based on personal health information, such as denial of medical insurance or employment. According to officials with the Office of the National Coordinator, the framework will continue to evolve as the office works with other federal agencies to further refine its goals, objectives, and strategies, which are described in appendix IV. While HHS continues to refine the goals and strategies of its framework for a national health IT strategy, it has not yet defined the detailed plans and milestones needed to ensure that its goals are met, as we previously recommended.

Legal Privacy Protections for Personal Health Information

As the use of electronic health information exchange increases, so does the need to protect personal health information from inappropriate disclosure. The capacity of health information exchange organizations to store and manage a large amount of electronic health information increases the risk that a breach in security could expose the personal health information of numerous individuals. According to results of a study conducted for AARP[14] in February 2006, Americans are concerned about the risks introduced by the use of electronic health information systems but also support the creation of a nationwide health information network. A 2005

[14]AARP is a nonprofit, nonpartisan membership organization for people age 50 and over.

Harris survey showed that 70 percent of Americans are concerned that an electronic medical record system could lead to sensitive medical information being exposed because of weak security, and 69 percent are concerned that such a system would lead to more personal health information being shared without patients' knowledge.[15] While information technology can provide the means to protect the privacy of electronically stored and exchanged health information, the increased risk of inappropriate access and disclosure raises the level of importance for adequate privacy protections and security mechanisms to be implemented in health information exchange systems.

Early Federal Laws Enacted to Protect the Privacy of Health Information

A number of federal statutes were enacted between 1970 and the early 1990s to protect individual privacy. For the most part, the inclusion of medical records in these laws was incidental to a more general purpose of protecting individual privacy in certain specified contexts. For example, the Privacy Act of 1974 was enacted to regulate the collection, maintenance, use, and dissemination of personal information by federal government agencies. It prohibits disclosure of records held by a federal agency or its contractors in a system of records[16] without the consent or request of the individual to whom the information pertains unless the disclosure is permitted by the Privacy Act or its regulations. The Privacy Act specifically includes medical history in its definition of a record. Likewise, the Social Security Act requires the Secretary of HHS to protect beneficiaries' records and information transmitted to or obtained by or from HHS or the Social Security Administration. Descriptions of these and other federal laws that protect health information are provided in appendix V.

Health Insurance Portability and Accountability Act of 1996

Federal health care reform initiatives of the early- to mid-1990s were, in part, inspired by public concern about the privacy of personal medical information as the use of health IT increased. Congress, recognizing that benefits and efficiencies could be gained by the use of information technology in health care, also recognized the need for comprehensive federal medical privacy protections and consequently passed the Health

[15]AARP Public Policy Institute; Goldman, Janlori; Stewart, Emily; and Tossell, Beth, Health Privacy Project, *The Health Insurance Portability and Accountability Act Privacy Rule and Patient Access to Medical Records*, 2006-03 (Washington, D.C.: February 2006).

[16]The Privacy Act defines a "system of records" as a group of records under the control of any agency that contains information about an individual and from which information is retrieved by the name of the individual or other personal identifier.

Insurance Portability and Accountability Act of 1996. This law provided for the Secretary of HHS to establish the first broadly applicable federal privacy and security protections designed to protect individual health care information. HIPAA provides for the protection of certain health information held by covered entities, defined under regulations implementing HIPAA as health plans that provide or pay for the medical care of individuals, health care providers that electronically transmit health information in connection with any of the specific transactions regulated by the statute, and health care clearinghouses that receive health information from other entities and process or facilitate the processing of that information into standard or nonstandard format for those entities.[17]

HIPAA requires the Secretary of HHS to promulgate regulatory standards to protect the privacy of certain personal health information.[18] "Health information" is defined by the statute as any information in any medium that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse and relates to the past, present, or future physical or mental health condition of an individual, provision of health care of an individual, or payment for the provision of health care of an individual. HIPAA also requires the Secretary of HHS to adopt security standards for covered entities that maintain or transmit health information to maintain reasonable and appropriate safeguards. The law requires that covered entities take certain measures to ensure the confidentiality and integrity of the information and to protect it against reasonably anticipated unauthorized use or disclosure and threats or hazards to its security.

HIPAA provides authority to the Secretary to enforce these standards. The Secretary has delegated administration and enforcement of privacy standards to the department's Office for Civil Rights and enforcement of the security standards to the department's Centers for Medicare and Medicaid Services.

[17]Transactions covered by the standards include enrollment and disenrollment in a health plan, eligibility determinations for a health plan, health care payment and remittance advice, premium payments, health claims information and claim status, coordination of benefits, and referral certification and authorizations.

[18]The statute requires the Secretary to issue standards for privacy and security. The standards issued by the Secretary are styled as rules. We use that terminology in this report.

Finally, most, if not all, states have statutes that in varying degrees protect the privacy of personal health information. HIPAA recognizes this and specifically provides that regulations implementing HIPAA do not preempt contrary provisions of state law if the state laws impose more stringent requirements, standards, or specifications than the federal privacy rule. In this way, HIPAA and its implementing rules establish a baseline of mandatory minimum privacy protections and define basic principles for protecting personal health information.

The Secretary of HHS first issued HIPAA's Privacy Rule in December 2000, following public notice and comment, but later modified the rule in August 2002. The Privacy Rule governs the use and disclosure of protected health information, which is generally defined as individually identifiable health information that is held or transmitted in any form or medium by a covered entity. The Privacy Rule regulates covered entities' use and disclosure of protected health information. In general, a covered entity may not use or disclose an individual's protected health information without the individual's authorization. However, uses and disclosures without an individual's authorization are permitted in specified situations, such as for treatment, payment, and health care operations and public health purposes. In addition, the Privacy Rule requires that a covered entity make reasonable efforts to use, disclose, or request only the minimum necessary protected health information to accomplish the intended purpose, with certain exceptions such as for disclosures for treatment and uses and disclosures required by law.

Most covered entities must provide notice of their privacy practices. Such notice is required to contain specific elements that are set out in the regulations. Those elements include (1) a description of the uses and disclosures of protected health information the covered entity may make; (2) a statement of the covered entity's duty with regard to the information, including protecting the individual's privacy; (3) the individual's rights with respect to the information, including, for example, the right to complain to HHS if he or she believes the information has been handled in violation of the law; and (4) a contact from whom individuals may obtain further information about the covered entity's privacy policies.

A covered entity is also required to account for certain disclosures of an individual's protected health information and to provide such an accounting to those individuals on request. In general, a covered entity must account for disclosures of protected health information made for

purposes other than for treatment, payment, and health care operations, such as for public health or law enforcement purposes.

HIPAA's Privacy Rule reflects basic privacy principles for ensuring the protection of personal health information. Table 1 summarizes these principles.

Table 1: Key Privacy Principles in HIPAA's Privacy Rule

HIPAA Privacy Rule principle	
Uses and disclosures	Provides limits to the circumstances in which an individual's protected health information may be used or disclosed by covered entities and provides for accounting of certain disclosures; requires covered entities to make reasonable efforts to disclose or use only the minimum necessary information to accomplish the intended purpose for the uses, disclosures, or requests, with certain exceptions such as for treatment or as required by law.
Notice	Requires most covered entities to provide a notice of their privacy practices including how personal health information may be used and disclosed.
Access	Establishes individuals' right to review and obtain a copy of their protected health information held in a designated record set.[a]
Security[b]	Requires covered entities to safeguard protected health information from inappropriate use or disclosure.
Amendments	Gives individuals the right to request from covered entities changes to inaccurate or incomplete protected health information held in a designated record set.[a]
Administrative requirements	Requires covered entities to analyze their own needs and implement solutions appropriate for their own environment based on a basic set of requirements for which they are accountable.
Authorization	Requires covered entities to obtain the individual's written authorization or consent for uses and disclosures of personal health information with certain exceptions, such as for treatment, payment, and health care operations, or as required by law. Covered entities may choose to obtain the individual's consent to use or disclose protected health information to carry out treatment, payment, or health care operations but are not required to do so.

Source: GAO analysis of HIPAA Privacy Rule

[a]According to the HIPAA Privacy Rule, a designated record set is a group of records maintained by or for a covered entity that are (1) the medical records and billing records about individuals maintained by or for a covered health care provider; (2) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (3) used, in whole or in part, by or for the covered entity to make decisions about individuals.

[b]The HIPAA Security Rule further defines safeguards that covered entities must implement to provide assurance that health information is protected from inappropriate uses and disclosure.

Subsequent to the issuance of the Privacy Rule, the Secretary issued the HIPAA Security Rule in February 2003 to safeguard electronic protected health information and help ensure that covered entities have proper security controls in place to provide assurance that the information is protected from unwarranted or unintentional disclosure. The Security Rule

includes administrative, physical, and technical safeguards and specific implementation instructions, some of which are required and, therefore, must be implemented by covered entities. Other implementation specifications are "addressable" and under certain conditions permit covered entities to use reasonable and appropriate alternative steps. Covered entities are required to develop policies and procedures for both required and addressable specifications.

The privacy and security rules require covered entities to include provisions in contracts with business associates that mandate that business associates implement appropriate privacy and security protections. A business associate is any person or entity that performs on behalf of a covered entity any function or activity involving the use or disclosure of protected health information. The rules require covered entities to obtain through formal agreement satisfactory assurances that their business associates will appropriately safeguard protected health information. The Security Rule also contains specific requirements for business associate contracts and requires that covered entities maintain compliance policies and procedures in written form. However, covered entities are generally not liable for privacy violations of their business associates, and the Secretary of HHS does not have direct enforcement authority over business associates.

HHS Has Initiated Actions to Identify Solutions for Protecting Personal Health Information but Has Not Defined an Overall Approach for Addressing Privacy

HHS and its Office of the National Coordinator for Health IT have initiated actions to identify solutions for protecting health information. Specifically, HHS awarded several health IT contracts that include requirements for developing solutions that comply with federal privacy and security requirements, consulted with the National Committee on Vital and Health Statistics (NCVHS) to develop recommendations regarding privacy and confidentiality in the Nationwide Health Information Network, and formed the American Health Information Community (AHIC) Confidentiality, Privacy, and Security Workgroup to frame privacy and security policy issues and identify viable options or processes to address these issues. The Office of the National Coordinator for Health IT intends to use the results of these activities to identify technology and policy solutions for protecting personal health information as part of its continuing efforts to complete a national strategy to guide the nationwide implementation of health IT. However, HHS is in the early stages of identifying solutions for protecting personal health information and has not yet defined an overall approach for integrating its various privacy-related initiatives and for addressing key privacy principles.

HHS's Contracts Are to Address Privacy and Security Policy and Standards for Nationwide Health Information Exchange

HHS awarded four major health IT contracts in 2005 intended to advance the nationwide exchange of health information—Privacy and Security Solutions for Interoperable Health Information Exchange, Standards Harmonization Process for Health IT, Nationwide Health Information Network Prototypes, and Compliance Certification Process for Health IT. These contracts include requirements for developing solutions that comply with federal privacy requirements and identify techniques and standards for securing health information.

HHS's contract for privacy and security solutions is intended to provide a nationwide synthesis of information to inform privacy and security policymaking at federal, state, and local levels. In summer 2006, the privacy and security solutions contractor selected 33 states and Puerto Rico as locations in which to perform assessments of organization-level privacy- and security-related policies and practices that affect interoperable electronic health information exchange and their bases, including laws and regulations. The contractor is supporting states and territories as they (1) assess variations in organization-level business policies and state laws that affect health information exchange, (2) identify and propose solutions while preserving the privacy and security requirements of applicable federal and state laws, and (3) develop detailed plans to implement solutions. The contractor is to develop a nationwide report that synthesizes and summarizes the variations identified, the proposed solutions, and the steps that states and territories are taking to implement their solutions. It is also to deliver an interim report to address policies and practices followed in nine domains of interest: (1) user and entity authentication, (2) authorization and access controls, (3) patient and provider identification to match identities, (4) information transmission security or exchange protocols (encryption, etc.), (5) information protections to prevent improper modification of records, (6) information audits that record and monitor the activity of health information systems, (7) administrative or physical security safeguards required to implement a comprehensive security platform for health IT, (8) state law restrictions about information types and classes and the solutions by which electronic personal health information can be viewed and exchanged, and (9) information use and disclosure policies that arise as health care entities share clinical health information electronically. These domains of interest address privacy principles for use and disclosure and security.

The standards harmonization contract is intended to identify, among other things, security mechanisms that affect consumers' ability to establish and manage permissions and access rights, along with consent for authorized

and secure exchange, viewing, and querying of their medical information between designated caregivers and other health professionals. In May 2006, the contractor for HHS's standards harmonization contract selected initial standards that are intended to provide security mechanisms. The initial security standards were made available for stakeholder and public comment in August and September, and the contractor's panel voted on final standards that were presented to AHIC in October 2006. AHIC accepted the panel's report and forwarded it to the Secretary for approval.

HHS's Nationwide Health Information Network contract requires four selected contractors to develop proposals for a nationwide health information architecture and prototypes of a nationwide health information network. The prototypes are to address privacy and security solutions, such as user authentication and access control, for interoperable health information exchange. In June 2006, HHS held its first nationwide health information network forum, at which more than 1,000 functional requirements were proposed, including nearly 180 security requirements for ensuring the privacy and confidentiality of health information exchanged within a nationwide network. The proposed functional requirements were analyzed and refined by NCVHS, and on October 30, 2006, the committee approved a draft of minimum functional requirements for the Nationwide Health Information Network, and sent it to HHS for approval. In January 2007, the four contractors are to deliver and demonstrate functional prototypes that are deployed within and across three or more health care markets and operated with live health care data using the same technology for information exchange in all three markets.

HHS's Compliance Certification Process for Health IT contract is intended to identify certification criteria for electronic health records, including security criteria. In May 2006, the Certification Commission for Health IT, which was awarded the contract, finalized initial certification criteria for ambulatory electronic health records[19] including 32 security criteria that address components of the security principle, such as controls for limiting access to personal health information, methods for authenticating users before granting access to information, and requirements for auditing access to patients' health records. To date, 35 electronic health records products have been certified based on these criteria. The commission is

[19]Ambulatory electronic health records are records of medical care that include diagnosis, observation, treatment, and rehabilitation that is provided on an outpatient basis. Ambulatory care is given to persons who are able to ambulate, or walk about.

currently defining its next phase of certification criteria for inpatient electronic health records.

The National Committee on Vital and Health Statistics Made Recommendations for Addressing Privacy and Security within a Nationwide Health Information Network

In June 2006, NCVHS, a key national health information advisory committee, presented to the Secretary of HHS a report recommending actions regarding privacy and confidentiality in the Nationwide Health Information Network. The recommendations cover topics that are, according to the committee, central to challenges for protecting health information privacy in a national health information exchange environment. The recommendations address aspects of key privacy principles including (1) the role of individuals in making decisions about the use of their personal health information, (2) policies for controlling disclosures across a nationwide health information network, (3) regulatory issues such as jurisdiction and enforcement, (4) use of information by non-health care entities, and (5) establishing and maintaining the public trust that is needed to ensure the success of a nationwide health information network. The recommendations are being evaluated by the AHIC work groups, the Certification Commission for Health IT, Health Information Technology Standards Panel, and other HHS partners.

In October 2006, the committee recommended to the Secretary of HHS that HIPAA privacy rules be extended to include other forms of health information not managed by covered entities. It also called on HHS to create policies and procedures to accurately match patients with their health records and to require functionality that allows patient or physician privacy preferences to follow records regardless of location. The committee intends to continue to update and refine its recommendations as the architecture and requirements of the network advance.

The American Health Information Community's Confidentiality, Privacy, and Security Workgroup Is to Develop Recommendations to Establish a Privacy Policy Framework

AHIC, a committee that provides input and recommendations to HHS on nationwide health IT, formed the Confidentiality, Privacy, and Security Workgroup in July 2006 to frame the privacy and security policy issues relevant to all breakthrough areas and to solicit broad public input to

identify viable options or processes to address these issues.[20] The recommendations to be developed by this work group are intended to establish an initial policy framework and address issues including methods of patient identification, methods of authentication, mechanisms to ensure data integrity, methods for controlling access to personal health information, policies for breaches of personal health information confidentiality, guidelines and processes to determine appropriate secondary uses of data, and a scope of work for a long-term independent advisory body on privacy and security policies.

The work group has defined two initial work areas—identity proofing[21] and user authentication[22]—as initial steps necessary to protect confidentiality and security. These two work areas address the security privacy principle. According to the cochairs of the work group, the members are developing work plans for completing tasks, including the definition of privacy and security policies for all of AHIC's breakthrough areas. The work group intends to address other key principles, including, but not limited to, maintaining data integrity and control of access. It plans to address policies for breaches of confidentiality and guidelines and processes for determining appropriate secondary uses of health information, an aspect o. the use and disclosure privacy principle.

[20]In May 2006, several of the AHIC work groups recommended the formation of an additional work group composed of privacy, security, clinical, and technology experts from each of the other AHIC work groups. The AHIC Confidentiality, Privacy, and Security Workgroup first convened in August 2006.

[21]Identity proofing is the process of providing sufficient information (e.g., identity history, credentials, documents) to establish and verify a person's identity. Identity proofing already takes place throughout many industries, including health care. However, a standard methodology does not exist.

[22]User authentication is the process of confirming a person's claimed identity, often used as a way to grant access to data, resources, and other network services. While a user name and password provide a foundational level of authentication, several other techniques, most notably two-factor authentication, have additional capabilities.

HHS's Collective Initiatives Are Intended to Address Aspects of Key Privacy Principles, but an Overall Approach for Addressing Privacy Has Not Been Defined

HHS has taken steps intended to address aspects of key privacy principles through its contracts and with advice and recommendations from its two key health IT advisory committees. Table 2 describes HHS's current privacy-related initiatives and the key HIPAA privacy principles that they are intended to address.

Table 2: Key HIPAA Privacy Principles and HHS's Initiatives Intended to Address Aspects of the Principles

Principle	HHS's initiative
Uses and disclosures: provides limits to the circumstances in which an individual's protected heath information may be used or disclosed by covered entities and provides for accounting of certain disclosures; requires covered entities to make reasonable efforts to disclose or use only the minimum necessary information to accomplish the intended purpose for the uses, disclosures, or requests, with certain exceptions such as for treatment or as required by law	• HHS's privacy and security solutions contractor is to provide a nationwide summary of statewide assessments of organization-level privacy- and security-related policies and practices that affect interoperable electronic health information exchange, along with proposed solutions and implementation plans. It is also to provide examples of potential areas for additional guidance under HIPAA. • Initial work of the AHIC privacy subgroup is to include work on guidelines and processes to determine appropriate secondary uses of data. • NCVHS recommended that individuals be given the right to decide whether they want to have personally identifiable electronic health records accessible via the Nationwide Health Information Network (NHIN), that disclosures be made based on role-based and contextual access criteria, and that HHS support efforts to convene a diversity of interested parties to design, define, and develop role-based and contextual access criteria appropriate for the network.
Notice: requires most covered entities to provide a notice of their privacy practices including how personal health information may be used and disclosed	• HHS's privacy and security solutions contractor is to provide a nationwide summary of statewide assessments of organization-level privacy- and security-related policies and practices that affect interoperable electronic health information exchange, along with proposed solutions and implementation plans. It is also to provide examples of potential areas for additional guidance under HIPAA. • NCVHS recommended that HHS require that individuals be provided with information and education to ensure that they realize the implications of their decisions as to whether to participate in the NHIN.
Access: establishes individuals' rights to review and obtain a copy of their protected health information held in a designated record set	• HHS's privacy and security solutions contractor is to provide a nationwide summary of statewide assessments of organization-level privacy- and security-related policies and practices that affect interoperable electronic health information exchange, along with proposed solutions and implementation plans. It is also to provide examples of potential areas for additional guidance under HIPAA.

(Continued From Previous Page)

Principle	HHS's initiative
Security: requires covered entities to safeguard protected health information from inappropriate use or disclosure	• HHS's NHIN contractors proposed functional requirements including nearly 180 security requirements for the NHIN prototypes. • HHS's standards harmonization contractor selected 30 information exchange standards, including 13 related to consumer empowerment. • The electronic health record certification contractor defined 32 security criteria for certifying ambulatory electronic health record products. • HHS's privacy and security solutions contractor is to provide a nationwide summary of statewide assessments of organization-level privacy- and security-related policies and practices that affect interoperable electronic health information exchange, along with proposed solutions and implementation plans. It is also to provide examples of potential areas for additional guidance under HIPAA. It is also to address nine domains of information security. • NCVHS recommended that HHS support the research and technology needed to develop contextual access criteria appropriate for application to electronic health records and inclusion in the architecture of the NHIN. • The AHIC Confidentiality, Privacy, and Security Workgroup defined two initial work areas—identity proofing and user authentication—as the initial steps necessary to protect confidentiality and security.
Amendments: gives individuals the right to request from covered entities changes to inaccurate or incomplete protected health information held in a designated record set	• HHS's privacy and security solutions contractor is to provide a nationwide summary of statewide assessments of organization-level privacy- and security-related policies and practices that affect interoperable electronic health information exchange, along with proposed solutions and implementation plans. It is also to provide examples of potential areas for additional guidance under HIPAA.
Administrative requirements: requires covered entities to analyze their own needs and implement solutions appropriate for their own environment based on a basic set of requirements for which they are accountable	• HHS's privacy and security solutions contractor is to provide a nationwide summary of statewide assessments of organization-level privacy- and security-related policies and practices that affect interoperable electronic health information exchange, along with proposed solutions and implementation plans. It is also to provide examples of potential areas for additional guidance under HIPAA. • Initial work of the AHIC privacy subgroup is to include work on policies for breaches of personal health information confidentiality. • NCVHS recommended that HHS develop a set of strong enforcement measures that produces high levels of compliance with the rules applicable to the NHIN on the part of custodians of personal health information, but does not impose an excessive level of complexity or cost; ensure policies requiring a high level of compliance are built into the NHIN architecture; ensure appropriate penalties be imposed for violations committed by any individual or entity; ensure that individuals whose privacy is breached are entitled to reasonable compensation; and, if necessary, amend the HIPAA Privacy Rule to increase the responsibility of covered entities to control the practices of business associates.
Authorization: requires covered entities to obtain the individual's written authorization or consent for uses and disclosures of personal health information with certain exceptions, such as for treatment, payment, and health care operations, or as required by law. Covered entities may choose to obtain the individual's consent to use or disclose protected health information to carry out treatment, payment, or health care operations but are not required to do so:	• HHS's privacy and security solutions contractor is to provide a nationwide summary of statewide assessments of organization-level privacy- and security-related policies and practices that affect interoperable electronic health information exchange, along with proposed solutions and implementation plans. It is also to provide examples of potential areas for additional guidance under HIPAA. • NCVHS recommended that individuals have the right to decide whether they want to have their personally identifiable electronic health records accessible via NHIN and that HHS should monitor the development of approaches for allowing individuals to opt in or opt out of participation. • Initial work of the AHIC privacy subgroup will also include work on guidelines and processes to determine appropriate secondary uses of data.

Source. GAO analysis of HHS data.

HHS has taken steps to identify solutions for protecting personal health information through its various privacy-related initiatives. For example, during the past 2 years HHS has defined initial criteria and procedures for certifying electronic health records, resulting in the certification of 35 IT vendor products. However, the other contracts have not yet produced final results. For example, the privacy and security solutions contractor has not yet reported its assessment of state and organizational policy variations. Additionally, HHS has not accepted or agreed to implement the recommendations made in June 2006 by the NCVHS, and the AHIC Privacy, Security, and Confidentiality Workgroup is in very early stages of efforts that are intended to result in privacy policies for nationwide health information exchange.

HHS is in the early phases of identifying solutions for safeguarding personal health information exchanged through a nationwide health information network and has therefore not yet defined an approach for integrating its various efforts or for fully addressing key privacy principles. For example, milestones for integrating the results of its various privacy-related initiatives and resolving differences and inconsistencies have not been defined, nor has it been determined which entity participating in HHS's privacy-related activities is responsible for integrating these various initiatives and the extent to which their results will address key privacy principles. Until HHS defines an integration approach and milestones for completing these steps, its overall approach for ensuring the privacy and protection of personal health information exchanged throughout a nationwide network will remain unclear.

The Health Care Industry Faces Challenges in Protecting Electronic Health Information

The increased use of information technology to exchange electronic health information introduces challenges to protecting individuals' personal health information. Key challenges are understanding and resolving legal and policy issues, particularly those resulting from varying state laws and policies; ensuring appropriate disclosures of the minimum amount of health information needed; ensuring individuals' rights to request access to and amendments of health information to ensure it is correct; and implementing adequate security measures for protecting health information. Table 3 summarizes these challenges.

Table 3: Challenges to Exchanging Electronic Health Information

Area	
Understanding and resolving legal and policy issues	• Resolving uncertainties regarding varying the extent of federal privacy protection required of various organizations • Understanding and resolving data-sharing issues introduced by varying state privacy laws and organization-level practices • Reaching agreement on organizations' differing interpretations and applications of HIPAA privacy and security rules • Determining liability and enforcing sanctions in cases of breach of confidentiality
Ensuring appropriate disclosure	• Determining the minimum data necessary that can be disclosed in order for requesters to accomplish their intended purposes • Obtaining individuals' authorization and consent for use and disclosure of personal health information • Determining the best way to allow individuals to participate in and consent to electronic health information exchange • Educating consumers so that they understand the extent to which their consent to use and disclose health information applies
Ensuring individuals' rights to request access and amendments to health information to ensure it is correct	• Ensuring that individuals understand that they have rights to request access and amendments to their own health information to ensure that it is correct • Ensuring that individuals' amendments are properly made and tracked across multiple locations
Implementing adequate security measures for protecting health information	• Determining and implementing adequate techniques for authenticating requesters of health information • Implementing proper access controls and maintaining adequate audit trails for monitoring access to health data • Protecting data stored on portable devices and transmitted between business partners

Source: GAO analysis of information provided by state-level health information exchange organizations, federal health care providers, and health IT professional associations

Understanding and Resolving Varying Legal and Policy Issues

Health information exchange organizations bring together multiple and diverse health care providers, including physicians, pharmacies, hospitals, and clinics that may be subject to varying legal and policy requirements for protecting health information. As health information exchange expands across state lines, organizations are challenged with understanding and resolving data-sharing issues introduced by varying state privacy laws. Differing interpretations and applications of the privacy protection requirements of HIPAA and other privacy laws further complicate the ability of health information organizations to exchange data and to determine liability and enforce sanctions in cases of breach of confidentiality.

Differing legal requirements for protecting health information introduce challenges to the ability to share health information among multiple stakeholders that may not be covered to the same extent by HIPAA's

privacy and security rules. Providers that are members of health information organizations are typically covered by the privacy and security requirements of HIPAA, but the information exchange organizations that provide the technology and infrastructure to conduct information exchange generally are not covered entities. Rather, they are usually thought of as business associates that are contractually bound through agreements with covered entities to provide protections to the health information that they manage but are not directly covered by the HIPAA privacy and security rules. An official with one health information exchange organization stated that he found it hard to determine if his organization was a covered entity or a business associate. In some cases, according to an official with a health information privacy professional association, health information exchange organizations may not even be business associates as defined by HIPAA. The differences between or uncertainty regarding the extent of federal privacy protection required of various organizations may affect providers' willingness to exchange patients' health information if they do not believe it will be protected to the same extent they protect it themselves. In June 2006, NCVHS recommended that, if necessary, HHS amend the HIPAA Privacy Rule to increase the responsibility of covered entities to control the practices of business associates.

The need to reconcile differences in varying state laws' privacy protection requirements introduces another widely acknowledged challenge to ensuring the privacy protection of health information exchanged on a nationwide basis. As health information exchange officials in states with strong privacy protections consider exchanging health information with organizations in other states, they will need to determine the extent to which they could share health information with organizations in states that have less stringent or no state-level laws and policies. For example, an official with one health information exchange organization described its state's privacy laws as being much more stringent than federal requirements, while a health information exchange official in another state told us that HIPAA's privacy requirements are the only laws that apply to the information exchanged by its organization. In this case, according to the official with the first organization, it would share more health information with providers in its own state than it would with providers in the other state because the other state's less stringent privacy protection laws would not provide a sufficient level of protection. HHS recognized that sharing health information among entities in states with varying laws introduces challenges and intends to identify variations in state laws that

affect privacy and security practices through the privacy and security solutions contract that it awarded in 2005.

Organizations also described another challenge associated with understanding and resolving legal and policy requirements for protecting electronic health information exchanged among multiple and diverse organizations. Differing interpretations and applications of the HIPAA privacy and security rules by providers and health information exchange organizations can result in disagreement about the data that can be exchanged and with whom the data can be shared. An official with one health information exchange described differing applications of HIPAA's security requirements that affect the way systems are administered and hinder the exchange of health information. For example, to protect individuals' information from inappropriate disclosure, the organization requires that the systems' list of users be forwarded to managers so that they can review roles and access rights at least annually. HIPAA's requirements do not specify protections at this level of granularity, so other organizations may not require this level of activity. This can create disagreements between organizations about the data that can be exchanged and with whom data can be shared if one organization does not administer access rights as strictly as another.

Health information exchange organizations described difficulties with determining liability and enforcing sanctions in cases of confidentiality breaches. As the number of health information exchange organizations increases and information is shared on a widespread basis, determination of liability for improper disclosure of information will become more important but also more difficult. For example, the Markle Foundation described problems with tracing the source of a privacy violation and determining the responsible entity.[23] Without such information, it becomes very difficult, if not impossible, to enforce sanctions for violations and breaches of confidentiality.

Ensuring Appropriate Disclosure

Several organizations described issues associated with ensuring appropriate disclosure, such as determining the minimum data necessary that can be disclosed in order for requesters to accomplish the intended

[23]The Markle Foundation is an organization that works to accelerate the use of emerging information and communication technologies to address critical public needs, particularly in the areas of health and national security.

purposes for the use of the health information. For example, dieticians and health claims processors do not need access to complete health records, whereas treating physicians generally do. According to VA officials, the agency's ability to ensure appropriate disclosure is further complicated by the fact that the Veterans' Benefits Act prevents disclosure of certain information, such as information related to HIV infection, sickle cell anemia, and substance abuse, which must be removed from individuals' health records before the requested information is disclosed. Additionally, VA's current manual process for determining the legal authority for disclosures and the minimum amount of information authorized to be disclosed is difficult to automate because of the complexity of various privacy laws and regulations.

Organizations also described issues with obtaining individuals' authorization and consent for uses and disclosures of personal health information. For example, health information exchange organizations may provide individuals with the ability to either opt in or opt out of electronic health information exchange. The opt-in approach requires that health care providers obtain the explicit permission of individuals before allowing their information to be shared with other providers. Without this permission, an individual's personal health information would not be accessible. The opt-out approach presumes that an individual's personal health information is available to authorized persons, but any individual may elect to not participate. Another approach taken by health information organizations simply notifies individuals that their information will be exchanged with providers throughout the organization's network.

Several organizations described difficulties with determining the best way to allow individuals to participate in and consent to electronic health information exchange. While the opt-in approach increases individual autonomy, it is more administratively burdensome than the opt-out approach and may result in fewer individuals participating in health information exchange. The opt-out approach is easier, less costly, and may result in greater participation in health information exchange, but does not provide the autonomy that the opt-in approach does. The notification approach is the simplest to administer but provides individuals no choice regarding participation in the organization's data exchange. In June 2006, NCVHS recommended to the Secretary of HHS that the department monitor the development of opt-in and opt-out approaches; consider local, regional, and provider variations of consent options; collect evidence on the health, economic, social, and other implications of opt-in and opt-out

approaches; and continue an open, transparent, and public process to evaluate whether a national policy on opting in or opting out is appropriate.

Organizations also described the need to effectively educate consumers so that they understand the extent to which their consent or authorization to use and disclose health information applies. For example, one organization stated that a request made to limit use and disclosure at one facility in a network may not apply to other facilities within the same network, but consumers may assume the limitations do apply to all facilities and not take steps to limit disclosure in those other facilities.

Ensuring Individuals' Rights to Request Access and Amendments to Health Information

As the exchange of personal health information expands to include multiple providers and as individuals' health records include increasing amounts of information from many sources, keeping track of the origin of specific data and ensuring that incorrect information is corrected and removed from future health information exchange could become increasingly difficult. Several organizations described challenges with ensuring that individuals have access to and the ability to amend their ow. health information and with ensuring that amendments are made and tracked throughout their information exchange organizations.

Officials with HHS's Indian Health Service described a challenge with ensuring that individuals' amendments to their own health information are properly made and tracked. Additionally, as individuals amend their health information, HIPAA requires that covered entities make reasonable efforts to notify or alert and send the corrected information to certain providers and other persons that previously received the individuals' information. Meeting this requirement was described as a challenge by officials with VA, and it is expected to become more prevalent as the numbers of organizations exchanging health information increases.

Officials with DOD described difficulties with ensuring that individuals' amendments to health information are distributed across multiple facilities within its network of medical facilities. The department is addressing this problem through the implementation of electronic health records and information management tools that track requests for amendments and their status. Additionally, an official with a professional association described the need to educate consumers to ensure that they understand their rights to request access to and amendments of their own health information to ensure that it is correct.

Implementing Adequate Security Measures for Protecting Health Information

Organizations described the adequate implementation of security measures as another challenge that must be overcome to protect health information. For example, health information exchange organizations described difficulties with determining and implementing adequate techniques for authenticating requesters of health information, such as the use of passwords and security tokens. User authentication will become more difficult as health information exchange expands across multiple organizations that employ different techniques. The AHIC Confidentiality, Privacy, and Security Workgroup recognized this difficulty and identified user authentication as one of its initial work areas for protecting confidentiality and security.

Implementing proper access controls, particularly role-based access controls, was also cited as a challenge to determining the information to which requesters may have access. Several organizations stated that maintaining adequate audit trails for monitoring access to health information is difficult but is necessary to ensure that information is adequately protected.

Organizations described problems introduced by the need to protect health information stored on portable devices and data transmitted between business partners. The use of laptops and other portable media by health information exchange employees presents a challenge to organizations since the data stored on these media should be encrypted to be secure. The VA is also faced with limitations related to the need to encrypt electronic health information shared with its business partners. According to VA officials, the agency and its business partners' solutions must be compatible in order to share the encrypted data, and VA's deployment of encryption solutions is limited. Encryption of data can be challenging, as organizations often must implement hardware and complex software technology to achieve adequate protection.

Conclusions

As the use of health IT and the exchange of electronic health information increases, concerns about the protection of personal health information exchanged electronically within a nationwide health information network have also increased. HHS and its Office of the National Coordinator for Health IT have initiated activities that, collectively, are intended to address aspects of key privacy principles. While progress has been made through the various initiatives, HHS has not yet defined an approach and milestones

for integrating its efforts, resolving differences and inconsistencies between them, and fully addressing key privacy principles.

As the use of health IT and electronic information exchange networks expands, health information exchange organizations are faced with challenges to ensuring the protection of health information, including understanding and resolving legal and policy issues, ensuring that the minimum information necessary is disclosed only to those entities authorized to request the information, ensuring individuals' rights to request access and amendments to health information, and implementing adequate security measures. These challenges are expected to become more prevalent as more information is exchanged and as electronic health information exchange expands to a nationwide basis. HHS's current initiatives are intended to address many of these challenges. However, without a clearly defined approach that establishes milestones for integrating its efforts and fully addresses key privacy principles and these challenges, it is likely that HHS's goal to safeguard personal health information as part of its national strategy for health IT will not be met.

Recommendation for Executive Action

We recommend that the Secretary of Health and Human Services define and implement an overall approach for protecting health information as part of the strategic plan called for by the President. This approach should (1) identify milestones and the entity responsible for integrating the outcomes of its privacy-related initiatives, including the results of its four health IT contracts and recommendations from the NCVHS and AHIC advisory committees; (2) ensure that key privacy principles in HIPAA are fully addressed; and (3) address key challenges associated with legal and policy issues, disclosure of personal health information, individuals' rights to request access and amendments to health information, and security measures for protecting health information within a nationwide exchange of health information.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from HHS's Assistant Secretary for Legislation. The Assistant Secretary disagreed with our recommendation. Throughout the comments, the Assistant Secretary referred to the department's comprehensive and integrated approach for ensuring the privacy and security of health information within nationwide health information exchange. However, an overall approach for integrating the department's various privacy-related initiatives has not been fully

defined and implemented. We acknowledge in our report that HHS has established a strategic objective to protect consumer privacy along with two specific strategies for meeting this objective: (1) support the development and implementation of appropriate privacy and security policies, practices, and standards for electronic health information exchange, and (2) develop and support policies to protect against discrimination from health information. Our report also acknowledges the key efforts that HHS has initiated to address this objective, and HHS's comments describe these and additional state and federal efforts. HHS stated that the department has made significant progress in integrating these efforts. While progress has been made initiating these efforts, much work remains before they are completed and the outcomes of the various efforts are integrated. Thus, we recommended that HHS define and implement a comprehensive privacy approach that includes milestones for integration, identifies the entity responsible for integrating the outcomes of its privacy-related initiatives, addresses key privacy principles, and ensures that challenges are addressed in order to meet the department's objective to protect the privacy of health information exchanged within a nationwide health information network.

HHS specifically disagreed with the need to identify milestones and stated that tightly scripted milestones would impede HHS's processes and preclude stakeholder dialogue on the direction of important policy matters. We disagree and believe that milestones are important for setting targets for implementation and informing stakeholders of HHS's plans and goals for protecting personal health information as part of its efforts to achieve nationwide implementation of health IT. Milestones are especially important considering the need for HHS to integrate and coordinate the many deliverables of its numerous ongoing and remaining activities. We agree that it is important for HHS to continue to actively involve both public and private sector health care stakeholders in its processes. HHS did not comment on the need to identify an entity responsible for the integration of the department's privacy-related initiatives, nor did it provide information regarding any effort to assign responsibility for this important activity. HHS neither agreed nor disagreed that its approach should address privacy principles and challenges, but stated that the department plans to continue to work toward addressing privacy principles in HIPAA and that our report appropriately highlights efforts to address challenges encountered during electronic health information exchange. HHS stated that the department is committed to ensuring that health information is protected as part of its efforts to achieve nationwide health information exchange.

HHS also disagreed with our conclusion that without a clearly defined privacy approach, it is likely that HHS's objective to protect personal health information will not be met. We believe that an overall approach is needed to integrate the various efforts, provide assurance that HHS's initiatives continue to address key privacy principles (as we illustrate in table 2 of the report), and to ensure that key challenges faced by health information exchange stakeholders are effectively addressed. HHS also provided technical comments that we have incorporated into the report as appropriate. HHS's written comments are reproduced in appendix VI.

In written comments, the Secretary of VA concurred with our findings, conclusions, and recommendation to the Secretary of HHS and commended our efforts to highlight methods for ensuring the privacy of electronic health information. VA also provided technical comments that we have incorporated into the report as appropriate. VA's written comments are reproduced in appendix VII.

DOD chose not to comment on a draft of this report.

As agreed with your offices, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days from the date on the report. At that time, we will send copies of the report to other Chairmen and Ranking Minority Members of other Senate and House committees and subcommittees that have authorization and oversight responsibilities for health information technology. We will also send copies of the report to the Secretaries of Defense, Health and Human Services, and Veterans Affairs. Copies of this report will also be made available at no charge on our Web site at www.gao.gov.

If you have any questions on matters discussed in this report, please contact me at (202) 512-6240 or David Powner at (202) 512-9286, or by e-mail at koontzl@gao.gov or pownerd@gao.gov. Contact points for our offices of Congressional Relations and Public Affairs may be found on the last page of this report. Other contacts and key contributors to this report are listed in appendix VIII.

Linda D. Koontz

Linda D. Koontz
Director, Information Management Issues

David A. Powner

David A. Powner
Director, Information Technology Management Issues

Appendix I

Objectives, Scope, and Methodology

The objectives of our review were to

- describe the steps the Department of Health and Human Services (HHS) is taking to ensure privacy protection as part of the national health information technology (IT) strategy and
- identify challenges associated with meeting requirements for protecting personal health information within a nationwide health information network.

To address our first objective, we analyzed information that we collected from agency documentation and through discussions with officials with HHS components and advisory committees that play major roles in supporting HHS's efforts to develop and implement a national strategy for health IT, including activities intended to ensure the protection of electronic health information exchanged within a nationwide health information network. Specifically, we reviewed and assessed privacy-related plans and documentation describing HHS's efforts to ensure privacy protection from HHS's Office of the National Coordinator for Health IT, Office for Civil Rights, Centers for Medicare and Medicaid Services and its Office for E-Health Standards and Services, and the Office of the Assistant Secretary for Planning and Evaluation. We also held discussions with and collected information from the American Health Information Community and the National Committee on Vital and Health Statistics, the Secretary's two primary advisory committees for health IT.

We reviewed information from the Office of the National Coordinator for Health IT on the description and status of its plans to address health information privacy as part of its national health IT strategy. We identified recommendations that the American Health Information Community and the National Committee for Vital and Health Statistics made to the Secretary of Health and Human Services regarding protecting the privacy of electronic health information. We also reviewed documentation about the scope and status of privacy-related work currently planned or being conducted under several of the Office of the National Coordinator's health IT contracts that support its efforts to develop and implement a national health IT strategy. We reviewed procedures for enforcing privacy and security laws related to the protection of health information (i.e., the Health Information Portability and Accountability Act [HIPAA] privacy and security rules) from the Office for Civil Rights and the Office of E-Health Standards and Services. We also reviewed involvement by HHS's Agency for Healthcare Research and Quality, the National Institutes of Health, the

Health Resources and Services Administration, the Substance Abuse and Mental Health Services Administration, and the Centers for Disease Control and Prevention in initiatives to ensure privacy protection related to the electronic exchange of health information within a nationwide health information network.

We mapped the HHS privacy-related activities we identified to key privacy principles in the HIPAA Privacy Rule. We identified HHS activities that addressed specific aspects of these principles to describe the extent to which HHS's privacy-related initiatives are intended to address key privacy principles.

To address the second objective, we analyzed documentation from and held discussions with officials from the federal agencies that provide health care services—the Departments of Defense and Veterans Affairs and the Indian Health Service—and representatives from selected state-level health information exchange organizations. We selected these organizations by conducting literature research and consulting with HHS and recognized health IT professional associations to identify existing health information exchange organizations. We initially identified more than 40 organizations and then conducted screening interviews to narrow the universe to 7 state-level health information exchange organizations that were actively exchanging health information electronically. To ensure that we identified challenges introduced by both federal privacy protection requirements and requirements that are more stringent than existing federal protections, we included states that do not have state laws that supersede federal requirements and states with privacy laws that are more stringent than federal laws. We selected state-level health information organizations from California, Florida, Indiana, Louisiana, Massachusetts, North Carolina, and Utah. We also included a telehealth network from Nebraska and a community health center network from Florida to ensure that we identified any privacy-related challenges unique to their health care IT environments. During interviews, we asked the health information exchange organizations to provide examples of challenges associated with protecting the privacy of health information that they encountered with the implementation of electronic health information exchange networks, along with challenges that they anticipated would be introduced by the nationwide health information exchange being proposed by HHS. We also held discussions with HHS officials with the Agency for Healthcare Research and Quality, the National Institutes of Health, the Health Resources and Services Administration, the Substance Abuse and Mental Health Services Administration, and the Centers for Disease Control and

Prevention to collect examples of challenges those organizations and their stakeholders face in attempting to address federal privacy and security requirements.

To gain further insight into the challenges organizations face in protecting privacy while exchanging electronic health information, we contacted representatives from nationally recognized health IT professional organizations. We held discussions with officials from the American Health Information Management Association, the American Medical Informatics Association, the eHealth Initiative, the Healthcare Information and Management Systems Society, the Markle Foundation, and the Public Health Informatics Institute to discuss challenges these organizations faced that are associated with protecting electronic health information. We also gathered relevant information about the challenges in protecting privacy within health information exchange from officials with the Health Privacy Project, the Vanderbilt Center for Better Health, Kaiser Permanente, and NHII Advisors, a health information consulting firm.

We reviewed and analyzed the information provided by the health information exchange organizations, federal health care providers, and professional associations to identify key challenges associated with the electronic exchange of personal health information throughout the health care industry. To characterize the challenges that we identified, we analyzed the specific examples of challenges and categorized them into four broad areas of challenges—understanding and resolving legal and policy issues, ensuring appropriate disclosures of health information, ensuring individuals' rights to access and amend health information, and implementing adequate security measures for protecting health information.

We conducted our work from December 2005 through November 2006 in the Washington, D.C., area in accordance with generally accepted government auditing standards.

Appendix II

Major Federal Health Care Programs

The following table includes the major federal programs that provide health care services for U.S. citizens, the number of beneficiaries for each program, and the cost of each program for 2004.

Table 4: Federal Programs

Federal agency	Program	Beneficiaries	Expenditure (dollars in billions)
HHS	Medicare	42 million elderly and disabled beneficiaries	$301.5
HHS	Medicaid	57.6 million low-income persons	297.5 (joint federal and state)
HHS	State Children's Health Insurance Program	6.8 million children	6.6 (joint federal and state)
HHS	Indian Health Service	1.8 million Native Americans and Alaska Natives	3.7
Veterans Affairs (VA)	Veterans Health Administration	5.2 million veterans	26.8
Department of Defense (DOD)	TRICARE Program	8.3 million active-duty military personnel and their families and military retirees	30.4
Office of Personnel Management (OPM)	Federal Employees Health Benefit Program	8 million federal employees, retirees, and dependents	27

Source HHS, VA, DOD, and OPM budget documents

Appendix III

HHS Health IT Contracts

The following table describes key health IT contracts awarded by the HHS Office of the National Coordinator for Health IT.

Table 5: HHS Health IT Contracts

Contract	Date awarded	Initial duration	Initial cost (in millions)	Extended duration	Additional cost (in millions)	Duration	Total cost (in millions)	Description
American Health Information Community Program Support	September 2005	1 year	$0.8	First option year	2.2	2 years	$3.0	To provide assistance to the National Coordinator in convening and managing the meetings and activities of the health care community to ensure that the health IT plan is seamlessly coordinated.
Standards Harmonization Process for Health IT	September 2005	1 year	3.2	Phase II 1 year	3.9	2 years	7.1	To develop and test a process for identifying, assessing, endorsing, and maintaining a set of standards required for interoperable health information exchange.
Compliance Certification Process for Health IT	September 2005	1 year	2.8	Phase II 1 year	2.9	2 years	5.7	To develop and evaluate a compliance certification process for health IT, including the infrastructure components through which these systems interoperate.
Privacy and Security Solutions for Interoperable Health Information Exchange[a]	September 2005	1½ years	17.2 (Increased by $6 million in August 2006 to include additional studies)	n/a	n/a	1½ years	17.2	To assess and develop plans to address variations in organization-level business policies and state laws that affect privacy and security practices that may pose challenges to an interoperable health information exchange.

(Continued From Previous Page)

Contract	Date awarded	Initial duration	Initial cost (in millions)	Extended duration	Additional cost (in millions)	Duration	Total cost (in millions)	Description
Nationwide Health Information Network Prototypes	November 2005	1 year	18.6 (4 contracts)	Base year extended by 3 months	4.4	1¼ years	23.0	To develop and evaluate prototypes for a nationwide health information network architecture to maximize the use of existing resources such as the Internet to achieve widespread interoperability among software applications, particularly electronic health records. These contracts are also intended to spur technical innovation for nationwide electronic sharing of health information in patient care and public health settings.
Measuring the Adoption of Electronic Health Records	September 2005	2 years	1.8	n/a	n/a	2 years	1.8	To develop a methodology to better characterize and measure the state of electronic health records adoption and determine the effectiveness of policies aimed at accelerating adoption of electronic health records and interoperability.
Gulf Coast Electronic Digital Health Recovery	September 2005	1 year	3.7	n/a	n/a	1 year	3.7	To plan and promote the widespread use of electronic health records and digital health information recovery in the Gulf Coast regions affected by hurricanes last year.

(Continued From Previous Page)

Contract	Date awarded	Initial duration	Initial cost (in millions)	Extended duration	Additional cost (in millions)	Duration	Total cost (in millions)	Description
State Alliance for e-Health	October 2006	1 year	1.9	n/a	n/a	1 year	1.9	To form a high-level steering committee that includes governors and state executives to identify and resolve issues that may present barriers to the formation of health information networks, including privacy, security, licenses and other legal issues, and health information exchanges.

Source: HHS Office of the National Coordinator for Health Information Technology.

[a]Jointly managed by the Agency for Healthcare Research and Quality and the Office of the National Coordinator.

Appendix IV

The Office of the National Coordinator for Health IT's Goals, Objectives, and Strategies

The following table describes the Office of the National Coordinators' current goals, objectives, and strategies and indicates which strategies are initiated, which are under active discussion, and which require future consideration.

Table 6: Goals, Objectives, and Strategies of the Office of the National Coordinator

Goal	Objective	High-level strategy
Goal 1: Inform health care professionals	High-value electronic health records	Simplify health information access and communication among clinicians[a]
		Increase incentives for clinicians to use electronic health records[c]
	Low-cost and low-risk electronic health records	Foster economic collaboration for electronic health records adoption[b]
		Lower total cost of electronic health records purchase and implementation[b]
		Lower risk of electronic health records adoption[a]
	Current clinical knowledge	Increase investment in sources of evidence-based knowledge[c]
		Increase investment in tools that can access and integrate evidence-based knowledge in the clinical setting[c]
		Establish mechanisms that will allow clinicians to empirically access information and other patient characteristics that can better inform their clinical decisions[c]
	Equitable adoption of electronic health records	Ensure low-cost electronic health records for clinicians in underserved areas[c]
		Support adoption and implementation by disadvantaged providers[c]
Goal 2: Interconnect health care	Widespread adoption of standards	Establish well-defined health information standards[a]
		Ensure federal agency compliance with health information standards[a]
		Exercise federal leadership in health information standards adoption[a]
	Sustainable electronic health information exchange	Stimulate private investment to develop the capability for efficient sharing of health information[b]
		Use government payers and purchasers to foster interoperable electronic health information exchange[c]
		Adapt federal agency health data collection and delivery to NHIN solutions[c]
		Support state and local governments and organizations to foster electronic health information exchange[b]
	Consumer privacy and risk protections	Support the development and implementation of appropriate privacy and security policies, practices, and standards for electronic health information exchange[a]
		Develop and support policies to protect against discrimination from health information[c]

(Continued From Previous Page)

Goal	Objective	High-level strategy
Goal 3: Personalize health management	Consumer use of personal health information	Establish value of personal health records, including consumer trust[b]
		Expand access to personal health management information and tools[a]
	Remote monitoring and communications	Promote adoption of remote monitoring technology for communication between providers and patients[a]
	Care based on culture and traits	Promote consumer understanding and provider use of personal genomics for prevention and treatment of hereditary conditions[c]
		Promote multicultural information support[c]
Goal 4: Improve population health	Automated public health and safety monitoring and management	Enable simultaneous flow of clinical care data to and among local, state, and federal biosurveillance programs[a]
		Ensure that the nationwide health information network supports population health reporting and management[c]
	Efficient collection of quality information	Develop patient-centric quality measures based on clinically relevant information available from interoperable longitudinal electronic health records[b]
		Ensure adoption of uniform performance measures by health care stakeholders[c]
		Establish standardized approach to centralized electronic data capture and reporting of performance information[c]
	Transformation of clinical research	No strategies identified
	Health information support in disasters and crises	Foster the availability of field electronic health records to clinicians responding to disasters[a]
		Improve coordination of health information flow during disasters and crises[c]
		Support management of health emergencies[c]

Source: HHS Office of the National Coordinator for Health IT.

[a]Strategy has been initiated.

[b]Strategy is under active consideration.

[c]Strategy requires future discussion.

Appendix V

Descriptions of Federal Laws for Protecting Personal Health Information

There are several federal statutes that protect personal health information. HIPAA provides the most extensive and specific protection. However, other federal statutes, although not always focused specifically on health information, nonetheless have the effect of protecting personal health information in specific situations. This table presents an outline of selected federal laws that protect personal health information.

Table 7: Selected Federal Laws that Protect Personal Health Information

Law	
HIPAA	
HIPAA administrative simplification provisions and regulations	Protected information: Certain individually identifiable health information transmitted by or maintained in electronic or any other form or medium by a covered entity.
	Protection provided: Disclosure of health information prohibited except as permitted by the Privacy Rule. The Security Rule requires that the security, integrity, and confidentiality of health information must be ensured.
	Applicability: Covered entities, which are defined as health plans, health care clearinghouses, and health care providers who transmit health information electronically in connection with authorized transactions.
Privacy protections applicable to federal government agencies	
Privacy Act of 1974	Protected information: Agency-controlled information about an individual that is retrieved by the individual's name or other personal identifier.
	Protection provided: Prohibits use and disclosure of personal records without consent of individual, or as otherwise permitted under the law; requires protection of personal records, disclosure of which could cause harm, embarrassment, unfairness, or inconvenience to the individual.
	Applicability: Executive agencies that hold information in a system of records (the law provides certain exceptions).
Freedom of Information Act of 1966	Protected information: Federal agency records.
	Protection provided: Act exempts from public release individually identifiable medical information, disclosure of which would constitute a clearly unwarranted invasion of personal privacy.
	Applicability: Executive federal agencies.

(Continued From Previous Page)	
Law	
Social Security Act	Protected information: Individually identifiable records and information held by an agency regarding program beneficiaries' records and information that is transmitted to, or obtained by or from HHS, Social Security Administration (SSA), and their contractors incident to carrying out agency duties.
	Protection provided: Prohibits unauthorized disclosure of individually identifiable records and makes unauthorized disclosure a crime.
	Applicability: HHS, SSA, and their contractors.
Veterans Omnibus Health Care Act of 1976	Protected information: Confidential medical records of treatment relating to the treatment of drug abuse, alcoholism or alcohol abuse, infection with the human immunodeficiency virus, or sickle cell anemia.
	Protection provided: Personally identifiable patient information provided or obtained in connection with treatment, education, evaluation, or research of certain conditions or diseases must be kept confidential, except with patient's written consent, or within VA, Department of Justice, or DOD.
	Applicability: VA.
Provisions protecting health information in limited situations	
Medicare Prescription Drug, Improvement, and Modernization Act of 2003	Protected information: Program beneficiaries' prescription drug, medication, and medical history information.
	Protection provided: Prescription drug plan sponsors must comply with HIPAA Privacy Rule and Security Rule requirements.
	Applicability: Prescription drug plan pharmacies and sponsors of prescription drug plans.
Clinical Laboratory Improvement Amendments of 1988	Protected information: Medical information of patients and clinical study subjects.
	Protection provided: Certain clinical laboratories are required to ensure confidentiality of test results or reports and may disclose such information only to authorized persons as defined by state or federal law.
	Applicability: Certain clinical laboratories conducting patient tests.
Public Health Service Act Health Omnibus Programs Extension of 1988	Protected information: Personal identifying information of individual subjects of biomedical, behavioral, clinical, or other research.

(Continued From Previous Page)

Law	
	Protection provided: The Secretary of HHS may issue a certificate of confidentiality to researchers engaged in biomedical, behavioral, clinical, or other research to protect any identifying research information from disclosure, including "compulsory legal demands".
	Applicability: Research programs.
Public Health Service Act Federal Confidentiality Requirements for Substance Abuse Patient Records	Protected information: Patient alcohol and drug abuse treatment records.
	Protected provided: Personally identifiable patient records maintained in connection with performance of drug abuse or substance abuse treatment must be kept confidential, absent patient consent or court order.
	Applicability: Federally assisted alcohol or substance abuse programs or activities.
Family Educational Rights and Privacy Act; Protection of Pupil Rights Amendment (covered education records are excluded under HIPAA's privacy and security regulations)	Protected information: Personally identifiable information in students' educational records; examination, testing, or treatment for mental or psychological conditions.
	Protection provided: Prohibits disclosure of protected information other than as needed within educational institution or by local or state educational agency, absent consent of parent, or student that has reached 18 years of age.
	Applicability: Educational institution or agency that receives federal funds under the Department of Education programs; educational institutions that conduct non-Department of Education-funded surveys.
Americans with Disabilities Act	Protected information: Medical information or condition and health records of employees or applicants.
	Protection provided: Covered entities must treat employees' and applicants' medical information as confidential medical records, with certain limitations as specified in the law.
	Applicability: Employers of 15 or more employees, employment agencies, labor organizations, and joint labor management committees.
Financial Modernization (Gramm-Leach-Bliley) Act of 1999	Protected information: Nonpublic personal information, which is defined as any nonpublic personal financial information provided by a consumer to a financial institution.
	Protection provided: Prohibits disclosure of consumers' nonpublic personal information to nonaffiliated third parties without clients' consent. (Consumers must be afforded the opportunity to decline the institution's sharing their information with nonaffiliated third parties.)
	Applicability: Financial institutions, including certain health insurers.

Source: GAO analysis of federal privacy laws

Appendix VI

Comments from the Department of Health and Human Services

DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Assistant Secretary for Legislation

Washington, D.C. 20201

DEC 29 2006

Ms. Linda D. Koontz
Director, Information Management Issues
U.S. Government Accountability Office
Washington, DC 20548

Dear Ms. Koontz:

Enclosed are the Department's comments on the U.S. Government Accountability Office's (GAO) draft report entitled, "HEALTH INFORMATION TECHNOLOGY: Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy" (GAO-07-238).

The Department has provided several technical comments directly to your staff.

The Department appreciates the opportunity to comment on this draft report before its publication.

Sincerely,

Rebecca Hernard

for Vincent J. Ventimiglia
Assistant Secretary for Legislation

COMMENTS FROM THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE U.S. GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO) DRAFT REPORT: HEALTH INFORMATION TECHNOLOGY: EARLY EFFORTS INITIATED BUT COMPREHENSIVE PRIVACY APPROACH NEEDED FOR NATIONAL STRATEGY (GAO-07-238)

General Comments

The Department of Health and Human Services (HHS) appreciates the opportunity to review the draft Government Accountability Office's (GAO) report entitled "HEALTH INFORMATION TECHNOLOGY – Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy."

HHS has established and is pursuing a deliberative, comprehensive, and integrated approach to ensure the privacy and security of health information within a nationwide health information technology (health IT) infrastructure. Although the GAO concludes otherwise, HHS continues to implement a "framework for strategic action," which it initially articulated in July 2004 and which continues to be a foundational guide for nationwide health IT adoption; and we fully believe that safeguarding personal health information is essential to our national strategy for health IT. The GAO draft report identifies numerous HHS projects, initiatives, and public-private collaborations underway that aggressively pursue the development of milestones for a nationwide health IT infrastructure premised on the privacy and security of health information; and while GAO concludes to the contrary, we believe the efforts highlighted in this report reflect HHS's comprehensive strategy to ensure that essential privacy and security protections are appropriately being integrated from the ground up into Federal solutions for interoperable health IT. In fact, the report's three recommendations well describe the activities HHS is currently engaged in to ensure the privacy and security of health information within a nationwide health IT infrastructure. Therefore, HHS does not concur with the GAO's conclusion that, "...HHS's goal to safeguard personal health information as part of its national strategy for health IT will not be met. (pg. 32)".

GAO's first recommendation calls on HHS to identify milestones and an entity responsible for the integration of outcomes related to our privacy-related initiatives. HHS believes that the tightly scripted milestones GAO recommends would impede our processes and preclude necessary public-private dialogue and input into the approach and direction on these important policy matters. Second, GAO recommends that HHS's approach "ensure that key privacy principles defined by HIPAA are fully addressed." The HIPAA Privacy Rule establishes a Federal floor of protections for health information held by most health care providers, health plans, and health care clearinghouses, while allowing States and organizations to provide greater protections as they see fit. This Rule and the HIPAA Security Rule establish the foundation principles of, and form the context in which, HHS continues to implement a comprehensive strategy for health IT privacy and security policy. Lastly, GAO recommends that our approach "address key challenges associated with legal and policy issues, disclosure of personal health information, patients' right to access and amend health information, and security measures for

2

protecting health information within a nationwide exchange of health information." The GAO report fittingly highlights the myriad complex collaborative efforts HHS is involved in to address the key challenges stated above. HHS is committed to ensuring that health information exchanged in nationwide network is protected.

HHS's strategy recognizes the importance of collaboration with both the public and private sectors, including representation from consumers of healthcare services. Many of our activities rely on public input, recommendations from Federal advisory committees, and deliverables from contracts with a wide variety of healthcare and IT sector collaborators, among other sources. Nationwide health IT adoption can only be accomplished through a coordinated effort of many stakeholders, within both state and Federal governments and the private sector. HHS has taken great care to engage representatives of all these sectors in our many health IT initiatives – an effort that involves many processes and the work of thousands of participants. Forging ahead with solutions that have not been informed by input from consumer groups and others in the private sector would deny these key stakeholders an opportunity to voice both their concerns and recommendations for solutions in this complex and sensitive policy area. Thus, creating tightly scripted milestones that do not provide an opportunity to be informed by such public-private dialogue would preclude the input necessary to inform the government's next steps. These processes are part of a comprehensive strategy for addressing complex technical and healthcare delivery issues; they advance the national health IT agenda, with all of its potential for improving healthcare and the health of the population; and effectively secure health information and the privacy of our citizens.

Overall, HHS's broad engagement in a full spectrum of contractual and other collaborative efforts reflect a well-structured, comprehensive and dynamic strategy that addresses key privacy and security principles. These activities indicate that HHS is very much on track to define solutions that will provide solid protection of health information while concurrently improving the quality of care through advancing the adoption of interoperable health IT.

HHS has invested significant resources and efforts on the nationwide strategy for protecting health information. Our national health IT agenda approaches privacy and security through a number of activities that both inform current work and prepare for future needs. As identified in this report, HHS already has a comprehensive portfolio of laws and activities to protect health information and define future needs for privacy and security protections as we move toward the President's vision for an interoperable health information technology infrastructure. HHS intends to draw upon these efforts to integrate privacy and security protections into meeting this vision. Our comprehensive strategy involves leveraging existing foundations, creating new public-private processes, partnering with states, health care organizations, and consumers to address state and business level protections, and considering privacy and security policies and implementation at a nationwide level. This multi-pronged, coordinated approach is designed to address each key element and constituent that will be required to enable a secure and consumer-focused nationwide transition to electronic health information exchange at all levels nationally. HHS efforts in each of these areas include:

3

Existing Foundations

HHS has promulgated several rules that establish Federal confidentiality, privacy, and security protections for health information, including the HIPAA Privacy and Security Rules, and the Confidentiality of Alcohol and Drug Abuse Patient Records Regulation. The Privacy Rule establishes a Federal floor of protections for health information held by most health care providers, health plans, and health care clearinghouses, while allowing States and organizations to provide greater protections as they see fit. These Rules establish the foundation principles of, and form the context in which HHS continues to implement a comprehensive strategy for, health IT privacy and security policy. Furthermore, HHS, like other agencies, must follow and implement the Privacy Act of 1974, which provides additional protections for records maintained by federal agencies.

State and Organizational Efforts

- *Privacy and Security Solutions for Interoperable Health Information Exchange*: Co-managed by the Agency for Healthcare Research and Quality (AHRQ) and the Office of the National Coordinator for Health IT (ONC), the Privacy and Security Solutions contract has fostered an environment where states and territories have been able to: (1) assess variations in organization-level business policies and state laws that affect health information exchange; (2) identify and propose practical solutions, while preserving the privacy and security requirements in applicable Federal and state laws; and (3) develop detailed plans to implement solutions to identified privacy and security challenges. These implementation plans will not only benefit the states and territories that have created them, but other ONC coordinated efforts such as the State Alliance for E-Health's Health Information Protection task force where interstate health information exchange issues can be harmonized nationwide.

- *State Alliance for E-Health*: Under contract with ONC, the National Governors Association will work with Governors and Governor-named high-level executives of states and U.S. territories to establish a high-level health IT advisory board. This body will be charged with identifying, assessing and, through the formation of consensus solutions, mapping ways to resolve state-level health IT issues that affect multiple states and pose challenges to interoperable electronic health information exchange; providing a forum in which states may collaborate so as to increase the efficiency and effectiveness of the health IT initiatives that they develop; and focusing on privacy and security issues surrounding the use and disclosure of electronic health information.

- *Development of Best Practices for State HIE Initiatives*: ONC has awarded a contract to the Foundation of Research and Education of the American Health Information Management Association (AHIMA) to gather information from existing state-level Health Information Exchanges and define, through a

4

consensus-based process, best practices that can be disseminated across a broad spectrum of healthcare and governmental organizations. Information was gathered related to governance, legal, financial and operational characteristics, and health information exchange policies. The contractor analyzed findings to develop guiding principles and practical guidance for state-level health information exchanges. AHIMA developed a work book and final report to disseminate guiding principles, and recommendations on how to encourage conformance and coordination across state and federal initiatives.

Federal Activities

- *American Health Information Community and Confidentiality, Privacy, and Security Workgroup*: In September 2005, the Secretary established the American Health Information Community (AHIC), a federally-chartered advisory committee made up of key leaders from the public and private sectors, charged with making recommendations to HHS on key health IT strategies. In the summer of 2006, the AHIC created a workgroup specifically focused on nationwide privacy and security issues raised by health IT activities and the findings of the other AHIC workgroups – privacy and security are one of the most consistent threads between each of the groups and their breakthrough projects. The first set of recommendations of this group will be presented to the AHIC in January 2007.

- *The Certification Commission for Healthcare Information Technology (CCHIT)*: In September 2005, ONC awarded a contract to CCHIT which was tasked with reducing barriers to the adoption of interoperable health information technologies through the creation of an efficient, credible and sustainable product certification program. The CCHIT membership includes a broad array of private sector representatives, including physicians and other healthcare providers, payers and purchasers, health IT vendors, and consumers. An important part of the task for CCHIT is to certify the security of health information systems. In each successive year, CCHIT will focus on security for ambulatory EHR systems, security for inpatient EHR systems and then security for network systems. The certification process CCHIT has developed promotes well-established, tested, security capabilities in health IT systems and certification will be a major contributor to protecting the privacy and confidentially of the data these systems manage.

- *Healthcare Information Technology Standards Panel (HITSP)*: In September 2005, ONC awarded a contract to the American National Standards Institute (ANSI) to identify standards for use in enhancing the exchange of interoperable health data. The process carried out by the Healthcare IT Standards Panel (HITSP) has created a unique and unprecedented opportunity to bring together the intellectual assets of over 260 organizations with a stake in health data standards that will increase the interoperability of healthcare systems and information.

5

A critical part of the HITSP mission is to harmonize the critical standards necessary to protect the privacy and security of health data. The panel guides the collaboration of its member organizations through a Health IT standards harmonization process that leverages the work and membership of multiple standards development organizations along with the expertise from the public and private sector. The panel engages in a consensus-based process to select the most appropriate standard from existing standards, where available, and to identify gaps in standards where there are none to assure effective interoperability. HITSP ensures that objections by interested parties are appropriately addressed and resolved, that the proceedings remain open to the public, that the industry's interests are adequately balanced, and further, that due process is followed with the ability of interested parties to appeal the panel's decisions. Once standards have been identified to support specific clinical use-cases, the HITSP will develop implementation guides to support system developers' activities in pursuing interoperable electronic health records.

- *Nationwide Health Information Network (NHIN)*: In November 2005, ONC awarded contracts to four consortia to develop prototypes capable of demonstrating potential solutions for nationwide exchange of health information. This initiative is foundational to the President's vision for the widespread adoption of secure, interoperable health records within 10 years. The prototype architectures developed will provide a framework for a public-private discussion on needed capabilities to support secure health information exchange across the nation. Each contract includes three geographically distinct healthcare markets. The output of the NHIN initiative includes prototype architectures that include functional requirements, business models, the identification of needed standards, and prototype software implementations. It is anticipated that this "network of networks" that will form the NHIN will be constructed from interoperable health information exchanges and sustainable markets for health information service providers.

A critical portion of the required NHIN deliverables is the development of security models that directly address systems architecture needs for securing and maintaining the confidentially of health data. Furthermore, each participant is required to comply with security requirements established by HHS to ensure proper and confidential handling of data and information and each is delivering important architecture capabilities that will be used in the next steps of the NHIN to address the complex issues of authentication, authorization, data access restrictions, auditing and logging, consumer controls of information access and other critical contributions.

SUMMARY

In summary, as the GAO report itself describes, HHS has made considerable progress integrating the activities and processes listed above into our overall strategy for ensuring privacy and security protections for health information in a health IT infrastructure. Each

6

activity and process involves many participants and organizations and will play a critical role in ensuring privacy and security of health information while advancing the adoption of health IT. Each activity and process has numerous deliverables and milestones. Many of our initiatives involve complex collaborative efforts and HHS seeks to be responsive to public comments and concerns while coordinating these public-private initiatives. HHS is focused directly on these privacy and security policy issues and is coordinating the integration of these policy issues through the health IT technology efforts presented.

7

Appendix VII

Comments from the Department of Veterans Affairs

THE SECRETARY OF VETERANS AFFAIRS
WASHINGTON

December 27, 2006

Ms. Linda D. Koontz
Director, Information Management Issues
Mr. David A. Powner
Director, Information Technology Issues
U. S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Koontz and Mr. Powner:

The Department of Veterans Affairs (VA) has reviewed your draft report, ***HEALTH INFORMATION TECHNOLOGY: Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy*** (GAO-07-238). I concur with the Government Accountability Office's (GAO) findings and conclusions. I support GAO's recommendations as they relate to the need for an overall approach that ensures key privacy principles and challenges associated with the nationwide exchange of health information are addressed fully.

However, the draft report mischaracterizes a situation in which an employee's computer equipment was stolen from the employee's home. Law enforcement officials subsequently recovered the equipment, which contained information on millions of veterans. After a thorough forensics assessment, Federal Bureau of Investigation officials stated publicly that they were "highly confident" that the veteran data were neither compromised nor accessed. It should be noted that the incident did not take place at the Veterans Health Administration level but at a Departmental level staff office, which was not a Health Insurance Portability and Accountability Act entity. While the context of GAO's report is privacy and security of health-related information, it should be noted that the data breach of personal information was not from a health care system of records.

In conclusion, I believe the report's effort to highlight methods of ensuring the privacy of electronic health information is commendable. The enclosure provides technical comments to enable more accuracy and clarity in GAO's report. VA appreciates the opportunity to comment on your draft report.

Sincerely yours,

R. James Nicholson

Enclosure

Appendix VIII

GAO Contacts and Acknowledgments

GAO Contacts

Linda D. Koontz, (202) 512-6240 or koontzl@gao.gov
David A. Powner, (202) 512-9286 or pownerd@gao.gov

Acknowledgments

In addition to those named above, Mirko J. Dolak, Amanda C. Gill, Nancy E. Glover, M. Saad Khan, Charles F. Roney, Sylvia L. Shanks, Sushmita L. Srikanth, Teresa F. Tucker, and Morgan F. Walts made key contributions to this report.

TESTIMONY OF MARK A. ROTHSTEIN
INSTITUTE FOR BIOETHICS, HEALTH POLICY AND LAW
UNIVERSITY OF LOUISVILLE SCHOOL OF MEDICINE

Before the

SUBCOMMITTEE ON FEDERAL GOVERNMENT MANAGEMENT, THE
FEDERAL WORKFORCE AND THE DISTRICT OF COLUMBIA

SENATE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS

Private Health Records: Privacy Implications of the
Federal Government's Health Information Technology Initiative

February 1, 2007

MR. CHAIRMAN and members of the Subcommittee. My name is Mark Rothstein. I am the Herbert F. Boehl Chair of Law and Medicine and Director of the Institute for Bioethics, Health Policy and Law at the University of Louisville School of Medicine. I am also Chair of the Subcommittee on Privacy and Confidentiality of the National Committee on Vital and Health Statistics, the statutory public advisory committee to the Secretary of Health and Human Services (HHS) on health information policy. I am testifying today in my individual capacity.

In my testimony today, I want to make only two points. First, HHS has made very little meaningful progress in developing and implementing measures to protect the privacy of health information in electronic health networks. Second, time is of the essence. HHS must begin to act immediately on the key privacy issues, and Congress needs to hold HHS accountable.

1. HHS and Health Privacy

I want to commend the Government Accountability Office (GAO) for its report, Health Information Technology. I believe this report accurately identifies the great challenges in adopting and integrating a comprehensive and effective strategy to protect health privacy, confidentiality, and security as the nation moves to a system of interoperable electronic health record networks.

I specifically agree with the following statement contained in the GAO report (p.14): "HHS is in the early stages of identifying solutions for protecting personal health information and has not yet defined an overall approach for integrating its various privacy-related initiatives and for addressing key privacy principles."

To this assessment, I would add my own view that privacy concerns currently lag behind technical development of the Nationwide Health Information Network (NHIN). Furthermore, I believe the gap is widening as research and development progress while fundamental privacy issues remain largely unexamined and unresolved.

The GAO report referred to the June 2006 letter to the Secretary of HHS from the National Committee on Vital and Health Statistics (NCVHS). The letter followed four public hearings across the country and the oral and written testimony of a wide range of experts and consumers from the U.S. and abroad. It took 18 months and a substantial amount of debate and deliberation among the diverse membership of the NCVHS. If nothing else, it has become very clear to those of us who worked on this letter that these issues are complicated, contentious, and crucial.

Here are just a few of the issues we considered:

- NCVHS noted that a decision is needed on whether individuals should have the option to participate in the NHIN and, if so, whether this choice should be through an opt-in, opt-out, or some other method.

- NCVHS raised the issue of whether individuals should have some control of the contents of their health records disclosed via the NHIN and, if so, how and over what health matters?
- NCVHS recommended that different levels of health information should be disclosed to different health care providers based on their need to know ("role-based access").
- NCVHS urged HHS to explore whether technology could be developed ("contextual access criteria") to limit the scope of disclosures when health information is divulged to employers, life insurers, and other entities that condition a financial or other relationship on access to an individual's health records.
- NCVHS clearly stated that health information privacy protections need to be comprehensive and extend beyond the current HIPAA covered entities "to all individuals and entities that create, compile, store, transmit, or use personal health information in any form and in any setting, including employers, insurers, financial institutions, commercial data providers, applications service providers, and schools."
- NCVHS stressed the importance of harmonizing all of the various federal statutes and regulations dealing with health privacy, incorporating fair information practices (e.g., rights of access, notice of disclosures) into the NHIN. implementing a vigorous enforcement system, and initiating public education programs to increase understanding of and build trust in the NHIN.

- In all, the letter contained 26 recommendations.

Unfortunately, HHS has not made any discernible progress on developing policies with regard to any of these foundational issues, either before or after the June 2006 letter. The privacy contracts let by HHS in 2005 primarily involve compiling and analyzing state privacy statutes and regulations that may be implicated by the adoption of electronic networks. The American Health Information Community working group dealing with privacy has concentrated on security issues, such as authentication and encryption. The four contractors selected by HHS to develop proposals for the NHIN architecture have not been required or encouraged to include new privacy enhancing technologies, such as contextual access criteria.

It is fair to conclude that health privacy has not received adequate attention at HHS, that prior efforts have lacked coordination and focused on the wrong issues, and that a sense of urgency is lacking.

2. Time is of the Essence

I cannot emphasize enough how rapidly the field of health information technology is moving. While HHS organizes more task forces and working groups, the private sector is racing ahead to implement a wide array of health information exchanges, medical record banks, regional health information organizations, and personal health record (PHR) systems. To take but one example, Wal-Mart and other large employers (Intel, BP, Pitney

Bowes, Allied Materials) with a total of 2.5 million employees in the U.S. recently announced that they are developing a PHR system for their employees (called Dossia) in an effort to improve employee health and lower employer health plan costs. Other large employers and health care provider networks are being recruited to form or join similar EHR and PHR alliances. Some of these networks already are operational.

It should be noted that these private sector initiatives with EHR and PHR networks are usually not subject to any federal or state regulation, because they are not covered entities under HIPAA. Furthermore, tens of thousands of other health care providers and health information providers are not covered entities under HIPAA. Most are not covered because they are not involved in the process of electronically submitting claims for health services.

What can be done to get HHS to put health information privacy on the fast track and the right track? I respectfully recommend that Congress condition continued appropriations for development of the NHIN on HHS demonstrating significant progress in addressing privacy issues. I also recommend that Congress play a greater role in oversight on this issue.

What would be "significant progress"? Clearly, HHS needs to address the 26 recommendations made to the Secretary in June 2006 by the NCVHS. (I have attached a copy of the letter and recommendations to my testimony.) The first order of business is for HHS to develop a draft framework for privacy and confidentiality in the NHIN. Then,

the public can participate in the deliberations about the framework. A variety of procedures can increase the level of public participation in this process, such as the following.

- HHS should publish a public request for information about key aspects of its privacy framework.
- HHH should hold a series of public hearings around the country on privacy issues.
- HHS should fund quantitative and qualitative research on public attitudes toward health information privacy.
- HHS should integrate key privacy principles into the NHIN architecture.
- HHS should publish an Advanced Notice of Proposed Rulemaking dealing with privacy in the NHIN.
- HHS should submit a report to Congress identifying gaps in coverage of the HIPAA Privacy Rule and how to address them.
- HHS should initiate public education programs on electronic health records (EHRs) and privacy protections.

MR. CHAIRMAN, I need not remind the members of the Subcommittee of the potential benefits of an effective and efficient NHIN, nor the dangers of an electronic health record system run amok. These issues are discussed in the GAO Report, the NCVHS letter, and elsewhere. One thing is certain. The health benefits of electronic health record networks will never be realized unless the American public has a high degree of trust in network privacy protections. We can't build the network and then build the trust. As the leader of

the NHIN-development effort, HHS must immediately begin to earn the confidence and trust of the American people through an expedited, coordinated, transparent, and public process of policy development leading to comprehensive, effective privacy protections.

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

PREPARED STATEMENT OF

CAROL C. DIAMOND, MD, MPH

MANAGING DIRECTOR, MARKLE FOUNDATION;

CHAIR, CONNECTING FOR HEALTH

Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia

Committee on Homeland Security and Governmental Affairs of the Senate of the United States

PRIVATE HEALTH RECORDS: PRIVACY IMPLICATIONS OF THE FEDERAL GOVERNMENT'S HEALTH INFORMATION TECHNOLOGY INITIATIVE

February 1, 2007

PREPARED STATEMENT OF
CAROL C. DIAMOND, MD, MPH
MANAGING DIRECTOR, MARKLE FOUNDATION;
CHAIR, CONNECTING FOR HEALTH

Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia
Committee on Homeland Security and Governmental Affairs of the Senate of the United States

PRIVATE HEALTH RECORDS: PRIVACY IMPLICATIONS OF THE FEDERAL GOVERNMENT'S HEALTH INFORMATION TECHNOLOGY INITIATIVE

February 1, 2007

Chairman Akaka, Senator Voinovich and distinguished members of the Subcommittee on Oversight of Government Management, thank you for inviting me to testify today. I am delighted to be called upon to share the Markle Foundation's insights on how information technology initiatives can enable the use of information to improve health care while protecting privacy. The report released by GAO summarizes well a number of issues regarding the current state of policy development for health information technology. Today I will address the implications of the current policy approach and propose a comprehensive privacy and security framework developed by the Markle Foundation's Connecting for Health collaboration. Our broad collaborative believes that such a Common Framework must be defined and maintained if we are to realize the goal of health information sharing environment that makes vital information available for patients and their

providers when and where it's needed, while protecting privacy and earning the trust of the American people.

THE MARKLE FOUNDATION: ADDRESSING CRITICAL PUBLIC NEEDS IN THE INFORMATION AGE

The Markle Foundation currently focuses on two areas where we believe expanded use of information technology (IT) and the improved use of information hold particular promise: the strengthening of our nation's security, and the modernization of our complex and over-burdened healthcare system. These are two of the most critical issues of our time, where the benefit to be gained from putting the right information in the right hands at the right time is enormous. In each of these areas, we know that the effective and appropriate use of IT can literally save lives. We also know that our nation's goals in both areas cannot be met without better use of IT[1].

At the same time, national security and healthcare also highlight a critical challenge we face in seeking new ways of using information: the need to protect our established values of privacy and civil liberties. Our commitment to designing new approaches to using and exchanging information must always be coupled with the development of policy and technology solutions that protect civil liberties and privacy from the outset, not as an afterthought.

If the policies and rules are not in place at the moment sensitive information, such as patient data, are collected and shared, public trust will be undermined, and in the process the very viability of electronic information collection and sharing will be threatened. In addition, we believe that these policies and business rules must be developed in a transparent, inclusive and

[1] The discussion of the objectives guiding the Markle Foundation work are based upon the 2004 letter by Zoë Baird, President of the Markle Foundation on **Addressing Critical Public Needs in the Information Age**. Available at http://www.markle.org/resources/president_letter/index.php

accountable manner; only this will ensure that the public accepts—and, indeed, embraces—new uses of technology as legitimate and desirable.

Markle has previously supported this Committee when it addressed the use of IT to improve information collection and sharing for national security purposes, while protecting critical privacy interests. Markle's Task Force on National Security in the Information Age[2], a distinguished panel of security experts spanning five administrations as well as experts on technology and civil liberties, developed a framework for improving our ability to share information while protecting privacy and civil liberties. To a significant extent, the President and Congress have now adopted a large set of recommendations suggested by the Task Force. Specifically, the Intelligence Reform and Terrorism Prevention Act of 2004, developed by this Committee and its leadership, Senators Joseph Lieberman and Susan Collins, grappled with these issues when it called for the creation of a trusted information sharing environment with Attributes and privacy policies encouraged by the Markle Task Force.

Many of the lessons learned and approaches taken by this Committee and its leadership in the national security area can also be applied to the focus of today's hearings: privacy and health information.

In the health area, we operate an initiative called Connecting for Health. Convened and operated by the Markle Foundation since 2002, Connecting for Health[3] works to accelerate the development of a health information-sharing environment to improve the quality and cost effectiveness of health care by bringing together private, public, and not-for-profit groups to develop common standards and policies. Together this group of leading government, industry, and health care experts have shaped and led the

[2] The Reports of the Markle Task Force on National Security in the Information Age are available at: http://www.markletaskforce.org/
[3] See http://www.connectingforhealth.org/

national debate on creating a health information-sharing environment that can make vital information available in a private and secure manner to improve the health and health care of all consumers.

In our 2004 Connecting for Health Roadmap[4], we recommended a decentralized and standards-based information network that is based on a framework of privacy and built on a model of trust, and identified a set of consensus actions to be taken by all healthcare stakeholders. In April 2006, this framework was fully documented and published, based on actual prototype implementation in Boston, Indianapolis and Mendocino County, California. The Connecting for Health Common Framework is based on a set of explicit privacy and technology principles and comprised of specific technology standards, health information policies, and model participation agreements. The model policies of the Common Framework were developed in and with the three prototype communities over the course of a year in parallel with the technical standards and architecture specifications. We convened both local stakeholders and the nation's leading experts in privacy, law, health information technology and health care delivery. The Common Framework is in the public domain and has been widely distributed and referenced[5].

The biggest lesson learned from participating in Connecting for Health for the last five years is now its guiding principle: that a sustainable environment for exchanging health information requires **technological design decisions to be developed in sync with policies and business rules that foster trust and transparency**[6].

---

[4] See **Achieving Electronic Connectivity In Healthcare**. A Preliminary Roadmap from the Nation's Public And Private-Sector Healthcare Leaders. Connecting for Health, July 2004. Available at http://www.connectingforhealth.org/resources/cfh_aech_roadmap_072004.pdf

[5] The **Common Framework** is available at http://www.connectingforhealth.org/commonframework/

[6] See **Keynote**, delivered by Zoe Baird at the Connecting Americans to Their Health Care Conference, December 8, 2006. Available at http://www.phrconference.org

We fully agree that technology and technical standards are crucial to realizing the benefits of health information sharing. But the government's greatest challenge is not finding the right technology or creating the most sophisticated technical infrastructure – it is finding agreement on the complex array of policies necessary for trustworthy information exchange. Computer systems that use the same technical standards will not move information by themselves for the care of a patient. Pushing the "send" button requires that the people who need to share information trust each other, understand and implement the necessary protections for the information they hold, and know that the information policies in place will be upheld and enforced in the event of a breach.

An explicit policy framework is as important as any effort to create technical standards. In health IT, technology standards by themselves are like an interstate highway system with no rules of the road. In order to serve the communities through which it passes, a highway must have a coherent set of rules, made obvious through signage and visibly enforced.

The converse is equally true: technology decisions made without clear information policies create information policy *de facto* - without public debate or agreement. Nowhere will this be more true than in the decisions regarding health information standards and prototype architectures for the Nationwide Health Information Network (NHIN). A design process that focuses purely on technology and standards will in fact also create health information policy. For example, decisions about where data should be stored or aggregated are also decisions about the kinds of risks to which data will be exposed. Choices among technical standards and architectures also determine whether personal health information is commingled with demographic data on the network as well as whether services and data are centralized. Make no mistake, these technical choices are all in fact health information policy decisions and they will all have implications for protecting privacy and

security. As with all significant policy decisions, the question of who has the authority to make the decision is as important as the initial policies themselves. In this case, policies that touch the most private concerns of every American can not simply be delegated to industry standard setting bodies. They must be made by a publicly accountable process. If technology is developed in advance of or in the absence of the relevant policy framework, our nation runs the risk of inappropriate uses of personal information followed by a public clamor for hasty remedies. In those circumstances, we may find ourselves retrofitting complex technologies at great costs. Experience tells us that these fixes will be inadequate, costly and operationally so difficult to implement that the policies may later be dismissed, delayed or modified because they cannot be realized. This unnecessary cycle will undermine the sustainability of a health information sharing network.

A better approach is to develop information policy alongside the technical system requirements. The challenge then is not a purely technical one. It's about finding the right technologies, standards and architectures that can implement the necessary policies to protect health information while allowing it to be shared with authorized parties.

AMERICANS SEE ELECTRONIC ACCESS TO THEIR MEDICAL INFORMATION AS A WAY TO IMPROVE QUALITY AND REDUCE HEALTH CARE COSTS IF THEIR SIGNIFICANT PRIVACY CONCERNS CAN BE ADDRESSED

If Government is unsure about the importance of these policies to the American public, it need only look at the years of public polling data that have been accumulated.

In December 2006, we released the results of a new survey on public views toward personal health records[7]. As in past years, our survey reveals a few key attitudinal themes regarding electronic personal health information. First, Americans want access to their personal health information electronically over the Internet for them and those who provide their care because they believe that the online services enabled by such access are likely to increase their quality of care. Additionally, the public sees online records as a way to increase health care efficiency by reducing unnecessary and repeated tests and procedures. A desire for more control over their health care also seems to be behind the public's interest in electronic personal health information. For instance: 97 percent think it's important for their doctors to be able to access all of their medical records in order to provide the best care; while 96 percent think it's important for individuals to be able to access all of their own medical records to manage their own health[8].

At the same time, Americans have significant **privacy concerns**, and will be reluctant to support health information exchange until these concerns are addressed in a comprehensive manner. Indeed, most respondents express concern that their medical information could be misused:

- 80 percent say they are very concerned about identify theft or fraud;
- 77 percent report being very concerned about their medical information being used for marketing purposes;
- 75 percent say the government has a role in establishing rules to protect the privacy and confidentiality of online health information;
- 66 percent say the government has a role in establishing rules by which businesses and other third parties can have access to personal health information; and

[7] Findings are available at http://www.markle.org/downloadable_assets/research_doc_120706.pdf
[8] Ibid.

- 69 percent say the government has a role in encouraging doctors and hospitals to make their personal health information available over the Internet in a secure way.

Our own surveys in the past and surveys done by others have repeatedly documented similar levels of concern:

- A Harris Interactive Survey on Medical Privacy[9] (February 2005) indicated that between 62% and 70% of adults are worried that sensitive health information might leak because of weak data security; that there could be more sharing of patients' medical information without their knowledge; that computerization could increase rather than decrease medical errors; that some people won't disclose necessary information to healthcare providers because of worries that it will be stored in computerized records; and that existing federal health privacy rules will be reduced in the name of efficiency.
- A California Health Care Foundation survey[10] (November 2005) indicated that 67% of Americans remain concerned about the privacy of their personal health information and are largely unaware of their rights.

These new risks require a comprehensive policy framework that builds privacy and security protections in from the start, rather than as post-hoc remedies. It is essential to realize that creating policies for information privacy is not a one-time effort. Information policies are no more static than technology developments; they must evolve with each new opportunity and innovation. Public trust cannot be fully accomplished by relying only on existing legal provisions such as the 1996 Health Insurance Portability and Accountability Act (HIPAA), which was created well before the advent of networked, portable health information systems and before any real

[9] Available at http://www.pandab.org/Healthtopline.pdf
[10] See http://www.chcf.org/topics/view.cfm?itemID=115694

contemplation of direct, or third party mediated electronic access to personal health information by consumers.

Some of the questions raised by GAO and with which this Committee will have to grapple include: how should these policies be developed? What is the appropriate level of oversight and public involvement? Who should have the authority to make these critical policy decisions? How will we ensure that a comprehensive policy framework applies to HIT efforts across government and within HHS, and to those in the private sector with which they interface? What are the key attributes that good information systems must uphold?

THE NEED FOR A COMMON POLICY AND TECHNOLOGY FRAMEWORK, BASED UPON PUBLIC INPUT

For the last three years, the Markle Foundation and 100 health stakeholders, from both the public and private health care sectors, the IT community and consumer advocates through the Connecting for Health Collaborative, have been developing consensus approaches toward information sharing. Our approach is based upon the shared belief that we must create **a Common Framework for secure, authorized, and private health information sharing**, so that patients and their authorized providers can have access to vital clinical data when and where they are needed.

The Connecting for Health *Common Framework* is specified in a set of 16 technical and policy guides developed by experts in information technology, health privacy law, health care delivery and policy. These guides were developed and tested in a working prototype in three different community settings in Indianapolis, Boston, and Mendocino County, California. The Common Framework specifies the necessary polices and technical standards for disparate health information networks to securely share information while protecting privacy and allowing for local autonomy and innovation.

THE ATTRIBUTES OF A COMMON FRAMEWORK

The Common Framework includes a set of Attributes that were identified to achieve the policy objectives of protecting privacy and building public trust.

I. Decentralized and Distributed Architecture

The health information sharing environment should not require the development of large centralized repositories of personal health information. Instead, it should be achieved by a decentralized "network of networks" based on common open standards with strong policy management and enforcement. The technical design was premised on leaving clinical data in the hands of those who have a direct relationship with the patient and leaving decisions about who should and should not see patient data in the hands of the patient and the physicians that are directly involved with his or her care.

II. Index that Separates Demographic from Clinical Information

Sharing information for the care of a patient from disparate information records should be accomplished with indices that show where relevant information resides but not what the information is. This approach does not require a unique patient identifier. Only those with proper authorization will then be allowed to access that information.

III. A Flexible Platform for Innovation

Creating a viable platform for innovation and new participants is critical to rapid evolution. The long-term value in an open set of standards and policies will be considerable in that it will create low barriers to entry, encourage innovation, maximize competition for privacy and security protections and reduce costs.

IV. Implement Privacy through Technology

Information technology tools should be developed and deployed to allow fast, easy, and effective implementation of our attributes for protecting privacy. These tools should create **audit trails** of who accesses the information, and prevent both the intentional and unintentional disclosure of information to unauthorized persons or entities by **building rules and permissions into the process** of accessing and distributing information. The approach to technology should create flexibility, implement strong security and promote data accuracy.

V. Nine Foundational Privacy Principles

The nine foundational privacy principles of the Connecting for Health Common Framework have been developed from the fair information practices as articulated within the United States Privacy Act and also from international privacy frameworks such as those developed internationally[11]. For each privacy principle, we suggested a corresponding question that points toward assessment criteria for e-health services:

1. **Openness and Transparency** *(Is it easy to understand what policies are in place, how they were determined, and how to make inquiries or comment? Is it clear who has access to what information for what purpose?)*

[11] The Committee should note that the questions it is considering today have also been considered by every other developed nation as it modernizes its health information systems. Our international colleagues, each working within their own political system and context, have come to very similar conclusions. They have conducted broad and transparent public discussions, prepared draft policies and subjected them to vigorous debate, and often altered their technical approach to address public concerns. The resulting policies – such as those summarized in the British "Care Record Guarantee" and the Australian 10 National Privacy Principles - lay out a national commitment to privacy in language that the public can understand. See http://www.connectingforhealth.nhs.uk/crdb/docs/crs_guarantee.pdf and http://www.privacy.gov.au/publications/chib.html

2. **Purpose Specification and Minimization** (*What is the purpose of gathering these data? Are the purposes narrowly and clearly defined?)*
3. **Collection Limitation** (*Are only those data needed for the specified purposes being collected, and are subjects fully informed of what is being collected?)*
4. **Use Limitation (***Will data only be used for the purposes stated and agreed to by the subjects?)*
5. **Individual Participation and Control** (*Can an individual find out what data has been collected and exercise control over whether and with whom it is shared?)*
6. **Data Integrity and Quality** (*How are data kept current and accurate?*
7. **Security Safeguards and Controls:** (*How are the data secured against breaches, loss or unauthorized access?)*
8. **Accountability and Oversight** (*Who monitors compliance with these policies and how is the public informed about violations?)*
9. **Remedies** (*How will complaints be handled, and will consumers be able to respond to or compensated for mistakes in decisions that are based upon the data?)*

Guided by these Attributes those who implement information networks can translate them into appropriate business rules, processes and practices that are embedded in a decentralized technical architecture and fine-tuned through public input and consultation. Considered and applied together, these attributes add up to an integrated and comprehensive framework to protect privacy. Together, they can help overcome the current fragmentation of policies and the evident consumer concern over privacy.

CONCLUSION

Today's hearing takes place at a unique moment. The President, the Secretary of Health and Human Services, AHIC, the National Health Information Technology Coordinator, and literally thousands of other actors are currently considering nationally, regionally and locally how to share health information using information technology.

Notwithstanding the current momentum and unified call for investment in health care information technology infrastructure, today we are missing a strong policy framework that would protect peoples' health information. Without the implementation of such a policy framework, accelerating the flow of health information could jeopardize the public's trust in a nationwide information exchange network. Current public concerns about identity theft and the broader dangers of breaches could lead to inadequate participation in health information sharing and a setback to our current window of opportunity to transform health care.

Congress, the administration and all parts of government have a critical role to play to ensure that personal health information can move where and when it's needed while also building public confidence in the privacy and security of our system. **Our key recommendations are**:

First, any government health information technology (health IT) initiative should be based on a privacy framework with the Attributes set forth in this testimony. Federally funded initiatives should be measured against metrics derived from each one of the Attributes of the framework.

Second, Congress is now considering the statutory authority of the Office of the National Coordinator for Health Information Technology (ONC) in the Department of Health and Human Services, the American Health Information

Community (AHIC) and other coordinating and oversight bodies. As it does so, it should appreciate that while these entities have been useful to initiate action in this field, we now need to determine the appropriate longer-term processes for making policy decisions and the technology determinations that implement them. Our national strategy for health IT must be executed by decision makers informed by, and accountable to, a broad range of interests—in particular decision makers that have direct public accountability. We must assure that all stakeholders and the American public are fully included in the policy and oversight processes. This should include an independent mechanism with high public visibility, to receive public complaints and handle disputes as appropriate such as the privacy officers, ombudsman or inspectors general that have been established for other purposes.

If we cannot accelerate the use of information technology for health information sharing, we will fail to address our health care challenges. We need the right policies to provide privacy and security, we need transparent oversight, and we need accountability.

I thank you for the invitation to appear. It has been a privilege to chair Connecting for Health, where so many dedicated individuals have worked together to recommend a Common Framework that accelerates the use of information to improve health and health care while protecting consumer privacy. I look forward to working with you to create a sustainable information-sharing environment for health care.

Thank you.
Carol C. Diamond

Appendix: Implementing the Nine Privacy Principles

Privacy Architectural Principles[12]	Policies and Procedures in a Networked Health Information Environment	Use of Technology for Privacy Protection[13]
Openness and Transparency *There should be a general policy of openness about developments, practices, and policies with respect to personal data. Individuals should be able to know what information exists about them, the purpose of its use, who can access and use it, and where it resides.*	– Transparency and tracking policies; – Collection and uses of personal data; – Adequate proper notice of privacy practices; – Disclosure procedures to individuals of security breaches; – Outreach and public education efforts to enhance awareness of privacy issues and privacy rights,	– Standards and technologies for expressing policies; – Standards and technologies for discovering policies once an institution's HIPAA provider number is known; – Defenses against people using transparency as an opportunity for phishing.[14]

[12] Considered and applied together, these principles add up to an integrated and comprehensive approach to privacy necessary for a connected health information exchange environment. **It is critical that the nine principles are considered as part of one package—elevating certain principles over others will simply weaken the overall architectural solution to privacy protection in a networked health information environment.**

[13] The use of technology for privacy protection depends to a large extent on the level of automatization of the envisaged process.

[14] Phishing is a tool used to gain personal information for purposes of identity theft. It involves using (fraudulent) e-mail messages that appear to come from legitimate businesses.

	as well as the risks and benefits of a networked environment.	
Purpose Specification and Minimization The purposes for which personal data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes or others that are specified on each occasion of change of purpose.	– Define acceptable uses of the system; – Define purposes of collection and of access for separate users such as: health care provider; health plan; public health authority; other government agency (law enforcement); researchers; individuals accessing their own health information; contractors and vendors (these might have a separate agreement); – Develop policies requiring that data collected for one purpose should not be used for another; – Implement a minimization requirement.	– Audit and logging technologies (including versioning); – Standards for expressing uses.

Collection Limitation Personal health information should only be collected for specified purposes, should be obtained by lawful and fair means and, where possible, with the knowledge or consent of the data subject.	– Define purposes of collection and of access for separate users such as: health care provider; health plan; public health authority; other government agency (law enforcement); researchers; individuals accessing their own health information; contractors and vendors (these might have a separate agreement).	– Separation of clinical and demographic information.
Use Limitation Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.	– Define acceptable uses of the system; – Decisions about linking and sharing are to be made by the participating institutions and providers at the edges of the network; – "User" limitation: different categories of users to be governed by different rules based upon separate use agreements; – Some data may not be shared because of special sensitivity (e.g., alcohol/drug abuse history, psychiatric treatment); – Patient authorization procedures need to be clarified and	– Technologies for de-identification; – Technologies for data aggregation; – Security to prevent unintended disclosures; – Limiting queries.

	streamlined; – Permitted disclosures need to be clarified (e.g., disclosure to health care providers for purposes of treatment, disclosure to health plans for payment); – Define reuse exceptions in cases of national security or law enforcement; – Use and disclosure for management and administration of Sub-Network Organizations (SNOs).	
Individual Participation and Control Individuals should control access to their personal information; *Individuals should be able to obtain from each entity that controls personal health data, information about whether or not the entity has data relating to them.* Individuals should have the right to:	– Patient authorization procedures; – Patient access to information procedures when information is: • Maintained by provider • Maintained by third party vendor; – User's responsibility w/r/t consent prior to sharing data; – Need for meaningful and clear patient control clauses that do not present "all or nothing" choices; – Consider ways to enhance patient control; – Clarify new liability issues arising from greater individual control;	– Differing degrees of control should be built into technology; – Users should be able to choose the level of control and necessary tradeoffs that are acceptable to them; – Defenses against phishing and data theft (through user authentication).

– *Have personal data relating to them communicated within a reasonable time (at an affordable charge, if any), and in a form that is readily understandable;* – *Be given reasons if a request (as described above) is denied, and be able to challenge such denial; and* – *Challenge data relating to them and have it rectified, completed, or amended.*	– Policies by which data may be withheld at direction of patient; – Requirement to draft consent and authorization forms in clear language, easily understandable to users.	
Data Integrity and Quality All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and current.	– Policies to ensure accuracy, consistency, and completeness of data; – Check their information and correct any errors (possibly model on Fair Credit Reporting Act); – Patient should be able to correct context of data use as well as content of data (i.e., they should	– Practices to ensure quality, accuracy, and availability, including backups, integrity checks, and periodic sampling; – Technical methods for allowing an individual to access and review his/her health record.

	be able to correct any misuse of data); – Clarify the SNO's liability in the case of: • Failure of the system to operate as expected or at all; • Loss or corruption of data within the system; • Incomplete or inaccurate data; • Misuse of the system by others, including other users; • Breach of security of the system.	
Security Safeguards and Controls Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure.	– Authorizing, managing, and policing access to information in the system by all categories of users; – Clear security policies (User's responsibility to implement reasonable and appropriate measures to maintain the security of the system and to notify the SNO of breaches in security, including any specific measures required by the SNO's policies and procedures); – Policies to handle intra- and extra-community matching	– Matching algorithm and thresholds; – Authentication of users; – Encryption technologies; – Auditing, service management, and logging.

	issues.	
Accountability and Oversight Entities in control of personal health data must be held accountable for implementing these information practices.	– Contract administration; – Policies by which the user has clear and sole responsibility for use of the system and actions taken in reliance on data in the system; – Consider mandating a position of Chief Privacy Officer (CPO) in organizations; – Clear user enrollment and termination procedures; – Designate someone responsible for ensuring patients' rights, such as access and amendment.	– Logging tools; – Auditing tools (including versioning); – Tracking systems; – Standards and technologies for allowing remote institutions to identify those accessing data at the individual level.
Remedies Legal and financial remedies must exist to address any security breaches or privacy violations.	– Policy and remedies for unauthorized disclosures.	– Web site with information about how patients can identify and pursue possible remedies.

Appendix: Connecting for Health, Steering Group Participants

Markle Foundation
Connecting for Health…A Public Private Collaborative
www.connectingforhealth.org
STEERING GROUP MEMBERSHIP (as of 12/06)

Antoine A. Agassi
Director and Chair
State of Tennessee eHealth Council

Peter A. Andersen, MD
Public Health and Clinical Informatics Officer, Relationship Manager
Lockheed Martin Corporation

Zoë Baird
President
Markle Foundation (ex-officio)

Robert B. Bogin, MD
Managing Director
Strategy and Collaborations Health Promotions Department
American Cancer Society

William Braithwaite MD
Former Senior Vice President and Chief Medical Officer
eHealth Initiative

Carolyn Clancy, MD
Director
Agency for Healthcare Research and Quality

Janet Corrigan, PhD
President and Chief Executive Officer
National Quality Forum

Mike Cummins
Chief Information Officer
VHA, Inc.

Mary Jo Deering, PhD
Director for Informatics Dissemination
Center for Bioinformatics
National Cancer Institute
National Institutes of Health, USDHHS

Carol Diamond, MD, MPH
Managing Director, Health Program
Markle Foundation
Chair, Connecting for Health

Colin Evans
Director, Policy and Standards
Digital Health Group, Intel Corporation

Mark Frisse, MD, MBA, MSc
Director, Regional Informatics
Vanderbilt Center for Better Health

Daniel Garrett
Former Vice President, Managing Partner, Global Health Solutions
Computer Sciences Corporation

J. Peter Geerlofs, MD
Chief Medical Officer
Allscripts Healthcare Solutions

John Glaser, PhD
Vice President and Chief Information Officer
Partners Healthcare System

Janlori Goldman JD
Director, Health Privacy Project

John Halamka, MD
Chief Information Officer
CareGroup Healthcare System

Linda Harris, PhD
Senior Health Communication Advisor
Office of Disease Prevention and Health Promotion
Office of the Secretary, HHS

Douglas Henley, MD
Executive Vice President
American Academy of Family Physicians

Joseph Heyman, MD
Trustee
American Medical Association

Gerald Hinkley, JD
Partner
Davis Wright Tremaine LLP

Yin Ho, MD
Director, eBusiness
Pfizer, Inc.

Kevin Hutchinson
Chief Executive Officer
SureScripts

Michael Jackman
Chief Technology Officer, Health Imaging
Eastman Kodak Company

William F. Jessee, MD
President and Chief Executive Officer
Medical Group Management Association

Y. Michele Kang
Vice President and General Manager, Health Solutions
Northrop Grumman Corporation

Michael L. Kappel
Senior Vice President, Government Strategy and Relations
McKesson Corporation

Brian F. Keaton, MD, FACEP
Attending Physician/EM Informatics Director
Summa Health System
President, American College of Emergency Physicians

Linda Kloss, RHIA, CAE
Executive Vice President and Chief Executive Officer
American Health Information Management Association

Allan M. Korn, MD, FACP
Senior Vice President, Clinical Affairs
Blue Cross Blue Shield Association

David Lansky, PhD
Senior Director, Health Program
Executive Director, Personal Health Technology Initiative
Markle Foundation

Stephen Lieber, CAE
President
Healthcare Information and Management Systems Society (HIMSS)

J. P. Little
Chief Operating Officer
RxHub, LLC

John R. Lumpkin, MD MPH
Senior Vice President, Director, Health Care Group
Robert Wood Johnson Foundation

Janet M. Marchibroda
Executive Director, Foundation for eHealth Initiative
Chief Executive Officer, eHealth Initiative

Howard Messing
President
Meditech, Inc.

Arnold Milstein, MD, MPH
Medical Director
Pacific Business Group on Health, The Leapfrog Group

Margaret O'Kane
President
National Committee for Quality Assurance

Dennis S. O'Leary, MD
President
Joint Commission on Accreditation of Healthcare Organizations

J. Marc Overhage, MD
President and Chief Executive Officer, Indiana Health Information Exchange
Associate Professor of Medicine, Indiana University School of Medicine
Senior Investigator, Regenstrief Institute

Herbert Pardes, MD
President and Chief Executive Officer
New York-Presbyterian Hospitals, University Hospitals of Columbia and Cornell
Vice Chair, Connecting for Health

Carol Raphael
President and Chief Executive Officer
Visiting Nurse Service of New York

Alison Rein
Assistant Director, Food and Health Policy
National Consumers League

Craig Richardson
Vice President, Health Care Strategy & Development
Johnson & Johnson Health Care Systems, Inc.

Wes Rishel
Vice President and Research Area Director
Gartner, Inc.

William Rollow, MD
Former Deputy Director, Quality Improvement Group
Office of Clinical Standards and Quality
Centers for Medicare and Medicaid Services

David Schulke
Executive Vice President
The American Health Quality Association

Steve Shihadeh
General Manager
Health Solutions Group
Microsoft, Inc.

Clay Shirky
Adjunct Professor
New York University
Graduate Interactive Telecommunications Program

Ellen Stovall
President
National Coalition for Cancer Survivorship

Thomas Sullivan, MD
Past President, Massachusetts Medical Society
Women's Health Center Cardiology
American Medical Association, Council on Medical Service
DrFirst.com Officer

Paul Tang, MD
Chief Medical Information Officer
Palo Alto Medical Foundation (PAMF), Sutter Health

Randy L. Thomas, FHIMSS
Associate Partner
Healthlink, a Division of IBM Corporation

Robin Thomashauer
Executive Director
Council for Affordable Quality Healthcare

John Tooker, MD, MBA, FACP
Executive Vice President and Chief Executive Officer
American College of Physicians

Micky Tripathi
Chief Executive Officer
Massachusetts eHealth Collaborative

Charlene Underwood, MBA
Director, Government and Industry Affairs
Siemens Medical Solutions

Scott Wallace
President and Chief Executive Officer
The National Alliance for Health Information Technology

Andrew Wiesenthal, MD
Associate Executive Director
The Permanente Federation

Marcy Wilder, JD
Partner
Hogan & Hartson LLP

Robert B. Williams, MD, MIS
Director, Healthcare Practice
Deloitte Consulting

Hugh Zettel
Director, Government and Industry Relations
GE Healthcare Integrated IT Solutions

June 22, 2006

Honorable Michael O. Leavitt
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Secretary Leavitt:

I am pleased to present you with a report of the National Committee on Vital and Health Statistics recommending actions regarding "Privacy and Confidentiality in the Nationwide Health Information Network." This report and its recommendations are the culmination of an 18 month process of learning and deliberation. The Subcommittee on Privacy and Confidentiality held three hearings in Washington, D.C., one in Chicago, and one in San Francisco. At each hearing, witnesses representing different constituencies concerned about the privacy and confidentiality of health information testified, including hospitals, providers, payers, medical informatics experts, ethicists, integrated health systems, Regional Health Information Organizations (RHIOs), and consumer and patient advocacy groups. We also heard testimony from representatives of nationwide health networks in Australia, Canada, and Denmark.

The hearings were followed by a series of conference calls and public meetings to discuss findings and prepare this report for the Committee to submit to HHS. Several times the Subcommittee presented its progress to the Committee and invited questions and comments. A thorough and animated discussion of the report at the full Committee meeting earlier this month culminated in approval.

The report covers several topics central to the challenges for safeguarding health privacy in the NHIN environment: the role of individuals in making decisions about the use of their personal health information, policies for controlling disclosures across the NHIN, regulatory issues such as jurisdiction and enforcement, use of information by non-health care entities, and establishing and maintaining the public trust that is necessary to ensure NHIN is a success. We hope that our analysis and recommendations will be valuable as the Department considers these important issues.

In presenting this report, the NCVHS acknowledges that the broad contour of the NHIN is still being determined. We will continue to update and refine these recommendations as the architecture and functional requirements of the NHIN advance.

We appreciate the opportunity to play a role in helping to shape the nation's health information policy.

Sincerely,

/s/

Simon P. Cohn, M.D., M.P.H.
Chairman, National Committee on
Vital and Health Statistics

Enclosure
Cc: HHS Data council Co-Chairs

PRIVACY AND CONFIDENTIALITY IN THE NATIONWIDE HEALTH INFORMATION NETWORK

The Nationwide Health Information Network (NHIN), on which the Department of Health and Human Services (HHS) is taking the lead, has the potential to enhance health care quality, increase efficiency, and promote public health. The NHIN also creates new challenges to and opportunities for safeguarding health privacy and confidentiality.

The National Committee on Vital and Health Statistics (NCVHS) has carefully considered the implications of the NHIN for health privacy and confidentiality. This report is based on a series of five hearings in 2005 held by the NCVHS Subcommittee on Privacy and Confidentiality. Three hearings were held in Washington, and one each in Chicago and San Francisco. Each hearing focused on different individuals and groups concerned about health information privacy and confidentiality, including hospitals, providers, payers, medical informatics experts, ethicists, integrated health systems, Regional Health Information Organizations (RHIOs), and consumer and patient advocacy groups. We also heard testimony from representatives of nationwide health networks in Australia, Canada, and Denmark. The Subcommittee then held a series of meetings open to the public and telephone conference calls to discuss its findings and prepare a report for the Committee to submit to HHS.

This report contains the following seven sections: (A) definitions; (B) the importance of privacy and confidentiality; (C) the role of individuals; (D) controlled disclosure of personal health information; (E) regulatory issues; (F) secondary uses of personal health information; and (G) establishing and maintaining public trust.

A. Definitions

One issue that often clouds discussions regarding privacy is the difficulty of differentiating among "privacy," "confidentiality," and "security." These terms are often used interchangeably and imprecisely. In this report, we have adopted definitions from the recent Institute of Medicine publication, "Disposition of the Air Force Health Study"

(2006). Health information privacy is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data. *Confidentiality*, which is closely related, refers to the obligations of those who receive information to respect the privacy interests of those to whom the data relate. *Security* is altogether different. It refers to physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure. Although a discussion of the appropriate security controls for the NHIN is beyond the scope of this report, security must be addressed for the NHIN to be successful. The security of electronic health records (EHRs) and the NHIN may be addressed in a future report of the NCVHS.

We use the term "personal health information" rather than "protected health information" because the latter is a term of art in the Privacy Rule promulgated under the Health Insurance Portability and Accountability Act (HIPAA), and we want to use a term not constrained by HIPAA coverage. The report also uses the term "individual" rather than "patient" in many places because not all health care providers (e.g., pharmacists) have a "provider-patient" relationship with the individuals they serve.

B. The Importance of Privacy and Confidentiality

Informational privacy is a core value of American society. Public opinion surveys consistently confirm the value of privacy to the public. Many individuals believe that there are certain matters that they do not want to share widely, or at all, even with friends, family members, or their physicians. Similarly, many people are quite concerned about the potential ramifications if employers, insurers, and other third parties have access to their personal information, including personal health information.

Privacy and confidentiality are neither new concepts, nor absolutes. Since the time of Hippocrates physicians have pledged to maintain the secrecy of information they learn about their patients, disclosing information only with the authorization of the patient or when necessary to protect an overriding public interest, such as public health. Comparable provisions are now contained in the codes of ethics of virtually all health professionals.

As a practical matter, it is often essential for individuals to disclose sensitive, even potentially embarrassing, information to a health care provider to obtain appropriate care. Trust in professional ethics and established health privacy and confidentiality rules encourages individuals to share information they would not want publicly known. In addition, limits on disclosure are designed to protect individuals from tangible and intangible harms due to widespread availability of personal health information. Individual trust in the privacy and confidentiality of their personal health information also promotes public health, because individuals with potentially contagious or communicable diseases are not inhibited from seeking treatment.

One of the major weaknesses of the current system of largely paper-based health records is its incomplete and fragmented nature. Ironically, this fragmentation has the unintended consequence of preventing disclosure of personal health information.

Precisely because comprehensive health information is difficult to access, compile, use, and disclose, some health information privacy and confidentiality may be achieved by default. Nevertheless, individuals pay dearly for this indirect protection in terms of unavailability of vital information in emergencies, difficulty in maintaining continuity of care, adverse health outcomes due to prescribing and other errors, waste of health care resources, and inability to compile aggregate data on health measures and outcomes. Thus, there are ample ethical, policy, and economic reasons for a shift to EHRs and an interoperable network of EHRs, so long as there are reasonable privacy and confidentiality measures.

People differ widely in their views regarding privacy and confidentiality, and individual opinions may be influenced by the individual's health condition as well as cultural, religious, or other beliefs, traditions, or practices. By providing individuals with reasonable choices concerning the uses and disclosures of their personal health information, the health care system and society demonstrate respect for persons. Furthermore, limiting excessive and unnecessary disclosure of personal health information helps to prevent health-based discrimination.

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

The NCVHS recognizes the difficulty in balancing the interests of privacy and confidentiality against the health care, economic, and societal benefits of the NHIN. Nevertheless, individual and societal interests are not necessarily inconsistent. There is a strong societal interest in privacy and confidentiality to promote the full candor on the part of the individual needed for quality health care. At the same time, individuals have a strong interest in giving health professionals the ability to access their personal health information to treat health conditions and safely and efficiently operate the health care system. Both the society as a whole and each individual have an interest in improvements in public health, research, and other uses of personal health information.

Throughout our hearings and in drafting this report and recommendations, it became clear to the members of the NCVHS that devising and establishing a NHIN involves difficult tradeoffs. As the availability of personal health information increases with new applications of technology, the utility of information increases, but so does the risk to privacy and confidentiality.

C. The Role of Individuals

The most difficult and contentious privacy and confidentiality issues are those surrounding whether and how individuals should have (1) choice over participation in the NHIN and (2) ability to control access to the contents of their health records accessible

over the NHIN. Addressing these difficult issues is further complicated because the specific structure of the NHIN has yet to be determined. For example, will the NHIN include storage of data, provide only the transport mechanism for moving data from place to place, or merely allow remote access to view data over a network? Without knowing the technical architecture or organizational plan of the NHIN, it is difficult to know what it means for an individual's records to be "accessible through" or "a part of" the NHIN.

1. Flexibility or uniformity?

Deciding on the appropriate level of individual control over personal health information accessible via the NHIN involves balancing important interests, such as the desire of some individuals to be able to control their personal health information and the need to document accurately medical history and treatment; the desire for a system that is flexible and the need to avoid a system that is too complicated; the desire to increase individual choice, and the desire to reduce complexity and the costs imposed on providers, payers, and other stakeholders.

Satisfying the desire of those who wish to promote individual choice and individual control suggests an NHIN with great flexibility. However, since there is a direct relationship between flexibility and complexity, too many choices could create a health information system that is overly complex, unwieldy to navigate, and needlessly expensive to design, implement, or operate. Too much flexibility might also result in individuals inadvertently withholding information necessary for appropriate treatment. Incomplete personal health information could jeopardize the improvement in individual and population health outcomes that provide a major justification for establishing the NHIN.

On the other hand, in an environment that lacks the flexibility to accommodate a variety of individual choices, privacy and confidentiality protections would be ineffectual. In such an environment, the public may be reluctant to support the establishment of the NHIN. Furthermore, individuals concerned about a lack of privacy and confidentiality might not disclose all relevant information to their health care providers, and some individuals might forego health care altogether.

An initial issue is whether individuals should have the right to continue having their personal health information maintained only on paper records. The NCVHS heard testimony on the issue from several witnesses. We conclude that although individuals should have reasonable control over the collection, use, and disclosure of their personal health information, the method by which their personal health information is stored by their health care providers should be left to the health care providers. Increasingly, records are being maintained in electronic form, and inevitably, that practice will continue and expand.

Recommendation

R-1 The method by which personal health information is stored by health care

providers should be left to the health care providers.

2. Mandatory or voluntary participation?

The next issue to consider is whether participation in the NHIN should be mandatory. The NCVHS believes that individuals should have a choice about whether to participate in the NHIN. Although we recognize that a system of mandatory participation would be easier, less costly, and more comprehensive, the Committee believes that these expected benefits do not justify the burden on individual privacy and confidentiality. In addition to the likely loss of political support if participation were mandatory, a loss of public health benefits is possible should individuals forego medical care because of privacy concerns. Accordingly, health care providers should not be able to condition treatment on individuals agreeing to have their health records accessible via the NHIN.

There are two basic approaches for giving individuals the choice of whether to have their personal health records accessible via the NHIN: opt-out and opt-in. Under the opt-out approach, an individual's personal health information is presumed to be available to authorized persons via the NHIN, but any individual may elect not to participate. The advantages of this approach are that it may be easier, less costly, and result in greater participation in the NHIN. The other approach, opt-in, requires that health care providers obtain the explicit permission of individuals before allowing their information to be available via the NHIN. Without this permission, an individual's personal health information would not be accessible via the NHIN. The opt-in approach increases individual autonomy, but is more administratively burdensome and may result in fewer individuals participating in the NHIN. While the NCVHS supports the principle of choice, we were unable to agree whether to endorse an approach as to how individuals should exercise this choice.

Under either approach, however, understandable and culturally sensitive information and education are needed to ensure that individuals realize the implications of electing or declining to participate. An individual's decision about participating in the NHIN should be the knowing exercise of an important right and not just another paper to sign to obtain health care.

Recommendations

R-2 Individuals should have the right to decide whether they want to have their personally identifiable electronic health records accessible via the NHIN. This recommendation is not intended to disturb traditional principles of public health reporting or other established legal requirements that might or might not be achieved via NHIN.

R-3 Providers should not be able to condition treatment on an individual's agreement to have his or her health records accessible via the NHIN.

R-4 HHS should monitor the development of opt-in/opt-out approaches; consider local, regional, and provider variations; collect evidence on the health, economic, social,

and other implications; and continue to evaluate in an open, transparent, and public process, whether a national policy on opt-in or opt-out is appropriate.

R-5 HHS should require that individuals be provided with understandable and culturally sensitive information and education to ensure that they realize the implications of their decisions as to whether to participate in the NHIN.

3. What is the nature of individual control?

Once an individual elects to make his or her information accessible via the NHIN, the next question is whether the individual should have the right to control access to specific portions of his or her record disclosed via the NHIN and, if so, the specifics of that right. NCVHS grappled with the question of whether the same rules regarding individuals' rights to control access to their health records accessible via the NHIN should also apply to the source of those health records originating with the health care provider. Although we describe below the arguments that the NCVHS heard on this matter during our hearings, NCVHS does not take a position on this issue. Nevertheless, we believe that this issue might become increasingly important.

Proponents of the view that individuals should not be permitted to control the contents of their health records raise three main arguments. First, they assert that such a policy is essential to maintain the integrity of the contents of the individual's health record. Current standard health information practices, some state laws, and widely adopted health professional standards require that any changes to the contents of a health record must be made through an amendment process and not by removing or deleting any information in the original record. Second, giving individuals the right to limit access to certain portions of their health record may interfere with the ability of their providers to make appropriately informed decisions. The concern is that individuals may not have the knowledge to discern what information in their health record can be blocked from access without affecting important decisions regarding their care. Third, NCVHS heard testimony from some health care providers who were concerned about possible malpractice liability stemming from errors in health care caused by accessing incomplete or filtered personal health information via the NHIN.

On the other hand, there are three main arguments in favor of granting individuals broader rights to control disclosure of their health records via the NHIN. First, proponents of this view assert that many health records contain sensitive, old information that is not relevant to a current clinical decision. Today, this information is often not available to all health care providers because of the fragmented nature of the health records system. However, under a functioning NHIN, sensitive, potentially embarrassing information would remain accessible indefinitely, possibly leading to stigma, humiliation, or even discrimination. This argument holds that a new health records system should not afford less protection for privacy and confidentiality than is presently afforded indirectly by the current, fragmented, largely paper-based system. In line with the tradition of a patient's right to control what treatments to accept or refuse, advocates of this position believe that individuals should have the right to withhold information, even if it may result in bad outcomes. Second, individuals with sensitive medical conditions, such as

substance abuse, mental illness, and sexually transmitted diseases, may be reluctant to seek treatment if they cannot be assured of controlling access to their personal health information. Thus, the argument is that individuals might forego treatment, thereby endangering their own or even the public's health. Third, NCVHS heard testimony that so long as health care providers have ready access to a standard set of essential information, such as current diagnoses, medications, allergies, and immunizations, emergency care can be rendered adequately and additional personal health information or permission to access additional personal health information can be obtained from the individual.

4. The degree of control

If individuals are given the right to control access to the contents of their health records, the next question is what degree of control should they have? Should they have the right to prevent access to any element in the record or only some elements? On the one hand, giving individuals unlimited control is one way to empower them. On the other hand, if individuals had unfettered control, health care providers would likely place less confidence in the accuracy and completeness of the records. A foreseeable result might be that instead of reducing duplication of effort, the new health record system could require every provider to obtain a new history and new individual information. Furthermore, most individuals would lack the expertise to determine which parts of their health record were relevant to current clinical decisions and would risk inadvertently excluding information to the detriment of their own health. For these reasons, if individuals are given the right to control access to their records, the right should be limited.

5. Methods of individual control

There are various ways in which individuals' rights to control access to their health records could be limited. For example, they could be based on the age of the personal health information (e.g., access could be denied only to records over 10 years old), they could be based on the nature of the condition or treatment (e.g., substance abuse, mental illness, reproductive health), and they could be limited by provider type or provider name. In developing a strategy for deciding to what type of information individuals should be permitted to limit access, it is important to consult with health care providers and patient advocates, including those representing culturally diverse populations.

Possible ways of affording individuals the right to control access to certain aspects of their health records include the following three proposals, none of which are necessarily endorsed by the NCVHS: (1) the entire records of a particular provider (e.g., psychiatrist) or a class of providers could be kept outside of the NHIN; (2) some parts of a health record could be blocked from access; or (3) some elements of a health record could be deleted altogether from the EHR. Blocking means that the information would still exist, but it will not be seen by health care providers looking at the record unless a provision for overriding blocked information (e.g., in emergencies) or granting certain providers access rights (e.g., allowing only mental health providers to see mental health information) is built into the system. Clinical decision support, however, might be

programmed to advise health care providers that, for example, the individual had a prior adverse reaction to a certain class of drugs. Blocked information also could be made available for statistical analyses, data aggregation, quality assurance, and other purposes in deidentified form. If a blocking approach were to be pursued, additional feasibility analyses would be necessary. Deletion carries with it the problems outlined in C.3. above.

The NCVHS heard testimony from experts about the Australian, British, Canadian, and Danish health systems, which grant individuals the right to block access to certain information. The Deputy Manager of the Danish Centre for Health Telematics testified that in Denmark, this right was rarely exercised, but individuals highly valued having this right. He further testified that he was not aware of any complaints by physicians about this arrangement. However, cultural, social, legal, or scalability differences may make the Danish experience inapposite.

Recommendations

R-6 HHS should assess the desirability and feasibility of allowing individuals to control access to the specific content of their health records via the NHIN, and, if so, by what appropriate means. Decisions about whether individuals should have this right should be based on an open, transparent, and public process.

R-7 If individuals are given the right to control access to the specific content of their health records via the NHIN, the right should be limited, such as by being based on the age of the information, the nature of the condition or treatment, or the type of provider.

D. Controlled Disclosure of Personal Health Information

Modern health care is often provided in large institutions with hundreds of employees in dozens of job categories. Not all of the individuals who need access to personal health information need the same level or kind of information. For example, dieticians and health claims processors do not need access to complete health records whereas treating physicians generally do. Protecting the confidentiality of personal health information in such settings requires institutions to establish different access rules depending on employees' responsibilities and their need to know the information to carry out their role. The HIPAA Privacy Rule includes a provision requiring that only the "minimum necessary" protected health information be included for disclosures other than for treatment, to the subject individual, pursuant to that individual's authorization, or where required by law. This minimum necessary standard encompasses role-based access. The principle of "role based access criteria" and the related concept of data classification have already been successfully embodied in the EHR architectures of several large health care organizations and health care systems. We support this principle and believe that it should be a standard for EHRs. We also believe that role based access criteria should be applied to the use and sharing of personal in the NHIN.

Another principle of controlled access applies to the non-medical uses of personal health information. Each year, as a condition of applying for employment, insurance,

loans, and other programs, millions of individuals are compelled to sign authorizations permitting employers, insurers, banks, and others to access their personal health information for non-medical purposes. These authorizations are nominally voluntary; individuals are not required to sign them, but if they do not, they will not be considered for the particular job, insurance policy, loan, or benefit. In addition, for most of these authorizations, no limits are placed on the scope of the information disclosed or the duration of the authorization. For example, after a conditional offer of employment, the Americans with Disabilities Act does not prohibit employers from requiring that individuals sign an authorization to release all of their health records, regardless of whether the information disclosed has any relevance to the position for which the individual is under consideration.

An EHR system creates greater risks to confidentiality because the comprehensive disclosures might include much more information than is necessary to the particular decision at hand. At the same time, conversion to EHRs creates an unprecedented opportunity to protect confidentiality. At present, it may not be practicable to search a paper record system to disclose only a certain category of personal. Thus, personal disclosed through compelled authorizations today is routinely overbroad, even where a narrower request is made. Conversion from paper records to EHRs could greatly enhance the confidentiality of personal health information and resolve the problem of excessive disclosures pursuant to authorizations. *Contextual access criteria* could be developed and integrated into the architecture of EHRs and the NHIN to permit disclosure of only the information needed by the user. For example, applying such technology, employers would only get information relevant to a particular job classification, and life insurers would only get information relevant to mortality risk. As a result, only personal relevant to its intended use would be disclosed pursuant to an authorization.

Developing the methodologies for these proposals will be complex and must involve collaboration by various stakeholders. The failure to incorporate contextual access criteria into the design of the NHIN, however, would have significant negative consequences, because this failure would impede the ability to limit unnecessary disclosures of irrelevant, sensitive personal to third parties. Despite our certainty that contextual access criteria are essential to protecting confidentiality in the NHIN, the NCHVS has been unable to identify any public or private research or pilot projects to develop this technology.

Recommendations

R-8 Role-based access should be employed as a means to limit the personal health information accessible via the NHIN and its components.

R-9 HHS should investigate the feasibility of applying contextual access criteria to EHRs and the NHIN, enabling personal information disclosed beyond the health care setting on the basis of an authorization to be limited to the information reasonably necessary to achieve the purpose of the disclosure.

R-10 HHS should support research and technology to develop contextual access criteria appropriate for application to EHRs and inclusion in the architecture of the NHIN.

R-11 HHS should convene or support efforts to convene a diversity of interested parties to design, define, and develop role-based access criteria and contextual access criteria appropriate for application to EHRs and the NHIN.

E. Regulatory Issues

The NHIN will require a series of regulatory measures to implement privacy and confidentiality protections. These measures fall into the categories of jurisdiction and relationship with other laws, procedures, and enforcement.

1. Jurisdiction, scope, and relationship with other laws

Several witnesses testified about the confusion, difficulty, and expense of complying with the HIPAA Privacy Rule along with numerous health privacy laws enacted by the states. Conflicts among the various sources of health privacy regulation would likely be even more pronounced with the NHIN. For example, what law would apply to an individual's health records created in states A and B, stored by or accessed through a RHIO in state C, disclosed to an entity in state D for use in state E? A single national standard would facilitate compliance, but the price of uniformity would be a loss in flexibility and the ability of the states to implement policies that reflect local conditions and values. NCVHS is aware that HHS has awarded a contract to the National Governors Association to study the variety of state laws regarding personal health information, and we look forward to the results of that effort. In the meantime, HHS should explore ways to preserve some degree of state variation without losing technical interoperability and essential protections for privacy and confidentiality.

Some of the privacy and confidentiality measures discussed in this report may be inconsistent with certain provisions of the HIPAA Privacy Rule. For example, under the Privacy Rule, individuals have a right to request amendments to their health records, but covered entities may refuse the request. In this report, we note that one option is to give individuals a right to exclude or block information contained in their EHR from being accessed via the NHIN. Adoption of this approach would require amendment of the Privacy Rule. In addition, the rules governing the NHIN need to be harmonized with other relevant federal regulations, including those applicable to substance abuse treatment records.

The purpose of the administrative simplification title of HIPAA was to regulate the process of submitting health care claims. Thus, the HIPAA Privacy Rule was designed to apply only to the covered entities involved in claims processing — health care providers, health plans, and health clearinghouses. Under the HIPAA Privacy Rule, protected health information may lose its protection after it travels from a covered entity to a non-covered entity. By contrast, the NHIN is designed to develop an interoperable infrastructure for coordinated, secure, personal exchange. The NHIN has a much broader scope and therefore, privacy and confidentiality rules must apply more broadly than is currently the case under the HIPAA Privacy Rule.

Recommendations

R-12 HHS should work with other federal agencies and the Congress to ensure that privacy and confidentiality rules apply to all individuals and entities that create, compile, store, transmit, or use personal health information in any form and in any setting, including employers, insurers, financial institutions, commercial data providers, application service providers, and schools.

R-13 HHS should explore ways to preserve some degree of state variation in health privacy law without losing systemic interoperability and essential protections for privacy and confidentiality.

R-14 HHS should harmonize the rules governing the NHIN with the HIPAA Privacy Rule, as well as other relevant federal regulations, including those regulating substance abuse treatment records.

2. Procedures

The NHIN would create a structure for disclosing sensitive information that previously was primarily controlled locally by health care professionals and health care administrators. Because the NHIN would represent a substantial change from current health information practices, the process of creating, implementing, and administering the NHIN must be open and transparent. HHS should encourage the input and participation of a broad cross-section of the population. The creation of the American Health Information Community (AHIC) is a valuable step in this direction. NCVHS will, in open and public sessions this summer, be reviewing an initial set of functional requirements for NHIN services. However, to ensure success, there is a continued need for regular, meaningful participation in the design and implementation of the NHIN by organizations, groups, and individuals affected by its creation. This participation must include members of medically vulnerable and minority populations.

Fair information practices should be incorporated into the NHIN. Some examples include the right to see an accounting of disclosures of one's record, the right to correct errors, and the right to a procedure for redress — investigation and resolution of complaints filed by individuals. An important information practice that has received significant attention in the press in the last year is how the system responds to incidents of unauthorized access to identifiable information, and whether the subjects of the unauthorized disclosure should be notified when the breach is discovered. That issue is very important to establishing the trust in the system, but the NCVHS has decided not to address the issue now, so that the specifics can be addressed in a separate letter dealing with security issues more broadly.

R-15 HHS should incorporate fair information practices into the architecture of the NHIN.

R-16 HHS should use an open, transparent, and public process for developing the rules applicable to the NHIN, and it should solicit the active participation of affected individuals, groups, and organizations, including medically vulnerable and

minority populations.

3. Enforcement

Several witnesses testified that strong enforcement and meaningful penalties are essential to deter wrongdoing and to assure the public that breaches of privacy, confidentiality, or security are taken seriously and will be dealt with aggressively. We believe that appropriate civil and criminal sanctions should be imposed on individuals and entities responsible for the violation of confidentiality and security provisions of EHRs and the NHIN. Under the HIPAA Privacy Rule, enforcement is in the hands of the Secretary, and an individual who is aggrieved must file a complaint with the Department to obtain relief under federal law. There is no private right of action. The Office for Civil Rights attempts to resolve those problems that lead to complaints directly with the covered entities, and we applaud the focus on improving the protections at the covered entity level. Nonetheless, prospective, general improvements by a covered entity often do not satisfy the individual who makes the complaint nor reassure the public that the law is being enforced adequately. A commitment to aggressive enforcement on the part of federal regulators is necessary to ensure the adoption and success of the NHIN.

There are many choices as to enforcement mechanisms that might be appropriate for the NHIN, including civil fines, revocation of licenses, withdrawal of membership rights, suspension or termination from participation in Medicare or Medicaid, payment of restitution, private rights of action, and criminal sanctions. These enforcement mechanisms might be imposed by legislation, regulation, contractual agreements, self-regulatory authorities, certifying or licensing boards, or other approaches. In the special case of unauthorized uses or disclosures in foreign jurisdictions, additional enforcement mechanisms might include international agreements on the protection of personal health information transmitted across national boundaries, limitations on the transmission of such information outside of the United States, or special licensing and registration requirements for foreign business associates. The success of the NHIN will depend on finding an appropriate suite of measures that produces high levels of compliance on the part of the custodians of individually identifiable information, but does not impose a level of complexity or cost that discourages investment.

NCVHS believes that, to date, the focus of the Department has been largely on developing infrastructure and generating investment. While both are critical, the Department should not neglect the policies and procedures that will control creation, collection, maintenance, use, disclosure, and eventual disposition of the information. A high level of enforcement is necessary to establish public confidence that privacy and confidentiality are properly protected. The NHIN also requires the widespread belief that its system of redress is responsive and fair. These policies cannot be created after the network is in place—by then it will be too late to impose new policies on an existing infrastructure. The policies must be built into the architecture from the beginning.

Among the enforcement principles for inclusion in the NHIN are the following: a wide range of penalties and sanctions should be available; penalties should be

progressive, with the most severe ones for willful and knowing violations, repeat offenders, or egregious wrongs; individuals should be entitled to some remedy for unlawful disclosures, including compensation for actual harm; establishing a new, federal private right of action should be avoided; and alternative dispute resolution should be encouraged.

Recommendations

R-17 HHS should develop a set of strong enforcement measures that produces high levels of compliance with the rules applicable to the NHIN on the part of custodians of personal health information, but does not impose an excessive level of complexity or cost.

R-18 HHS should ensure that policies requiring a high level of compliance are built into the architecture of the NHIN.

R-19 HHS should adopt a rule providing that continued participation in the NHIN by an organization is contingent on compliance with the NHIN's privacy, confidentiality, and security rules.

R-20 HHS should ensure that appropriate penalties be imposed for egregious privacy, confidentiality, or security violations committed by any individual or entity.

R-21 HHS should seek to ensure through legislative, regulatory, or other means that individuals whose privacy, confidentiality, or security is breached are entitled to reasonable compensation.

F. Secondary Uses

Many individuals are concerned about the disclosure of their confidential personal health information because of possible embarrassment, emotional distress, and stigma. They are also concerned about more tangible harms, such as the inability to obtain employment, mortgages and other loans, or various forms of insurance. Measures to protect the security of personal health information from unauthorized access and to protect the confidentiality of disclosures through fair information practices are extremely important. Nonetheless, these measures will only have a limited effect in addressing the public's primary concern about health "privacy" — the use of personal health information to adversely affect individuals' personal, financial and professional rights, interests, and opportunities.

1. Limitation on uses by third parties

In Section D, we discussed the importance of building into the architecture of the NHIN the capacity to use contextual access criteria to limit the scope of personal health information when disclosure is made to third parties pursuant to an authorization. The ability of holders of personal health information to limit disclosures to relevant information solves only part of the problem. Third party users of personal health information should be restricted to requiring authorization only for relevant personal health information. Furthermore, any personal health information obtained by a third

party in a context outside of the healthcare system should not be used unfairly to adversely affect an individual's personal, financial, or professional rights, interests, or opportunities.

All of these elements are essential to meaningful protection of individual privacy. Without information technology capable of protecting information from inappropriate disclosures, restricting access or use by third parties will be meaningless and without practical effect. At the same time, without appropriate restrictions to prevent third parties from obtaining or using personal health information in a context incompatible with individuals' expectations of appropriate use of their personal health information, third parties could evade the contextual access criteria of EHRs and the NHIN by simply demanding that individuals provide copies of records at the time of application for employment, loans, or insurance. Undoubtedly, the more often personal health information is available in a context outside of healthcare delivery, the more likely individuals will be unfairly discriminated against. NCVHS urges the Secretary to pursue legislative or regulatory measures designed to eliminate or reduce as much as possible the potential discriminatory effects of personal health information disclosures beyond health care.

Recommendation

R-22 HHS should support legislative or regulatory measures to eliminate or reduce as much as possible the potential harmful discriminatory effects of personal health information disclosure.

2. Relationship to the HIPAA Privacy Rule

More effective control of personal health information will require reconsideration of several key provisions of the HIPAA Privacy Rule. For example, under the current Privacy Rule, covered entities have limited responsibilities and limited recourse in oversight of the privacy and confidentiality procedures of business associates. When the Privacy Rule was promulgated, HHS recognized the business associate relationship and imposed some limitations to protect the privacy of financial transactions, but the current rule is inadequate to deal with relationships in which personal health information is shared directly between covered entities and their business associates. If the Privacy Rule is not amended, the new system of EHRs and the NHIN would permit domestic and overseas business associates to be able to obtain much more personal health information without any more oversight. Indeed, in the case of overseas associateships, which are increasing in the commercial marketplace, understanding or controlling the use of information may be particularly difficult.

Another area of concern involves the redisclosure of personal health information obtained by third parties pursuant to an authorization. Once information has been obtained by the commercial entity, it is not protected by the Privacy Rule. These and similar issues have been addressed in prior recommendations by the NCVHS, and the

more comprehensive disclosures via the NHIN make action on these recommendations imperative.

The HIPAA Privacy Rule was based on a "chain of trust" model, permitting information to flow freely among those involved directly in treatment, payment, or health care operations. However, an interoperable information sharing environment for personal health information will increase the amount of information that can flow to parties not originally contemplated by the Privacy Rule, i.e., those outside of the realm of treatment, payment, and health care operations. As information flows away from the people and organizations that collect and use it for its primary purpose, health care delivery, it becomes increasingly difficult to understand or control how it is being used for secondary or even tertiary purposes. Therefore, before moving to the NHIN, it is essential to tighten the gaps in the Privacy Rule that permit information to leak and to adopt a more comprehensive privacy protection regime.

Recommendation

R-23 NCVHS endorses strong enforcement of the HIPAA Privacy Rule with regard to business associates, and, if necessary, HHS should amend the Rule to increase the responsibility of covered entities to control the privacy, confidentiality, and security practices of business associates.

G. Establishing and Maintaining Public Trust

The NCVHS heard testimony that Americans are unsure whether the benefits of an NHIN outweigh the privacy risks, concerned about security of their information, and lacking in confidence about federal regulation. NCVHS observed that members of the public lack knowledge and understanding about what records exist about them, how they are used and shared, and what rules apply. There are also few opportunities for public participation in developing national health information policy. Consequently, public trust is lacking as we develop the NHIN.

The public concerns about EHRs and the NHIN make it essential that HHS and other public and private entities begin immediate, substantial, and sustained efforts to establish and maintain public trust in the NHIN. Maintaining a high level of public trust must be a key consideration of all associated with developing the NHIN. HHS must pursue three simultaneous courses to succeed at this goal. First, HHS must ensure that individuals understand what they stand to gain with the advent of the NHIN, and receive a fair assessment of the risks. At a time when media reports are much more likely to focus on rare security breaches than the everyday health benefits of EHRs, a major effort in public and professional education is essential. The NHIN cannot be imposed on the public; the public must be informed about the NHIN's weaknesses and strengths, risks and benefits, and become convinced of its merits.

What will convince the public? NCVHS finds that the one benefit that will win over public support is better health care. If we expect individuals to support an

interoperable network that permits quick and easy data sharing, the indispensable requisite must be a measurable improvement in the quality of individual care. During our hearings on the NHIN, one witness suggested that for its first five years of operation, the NHIN should be used exclusively for patient care, and only after public trust in the system is established would the system be available for quality assurance, outcomes research, syndromic surveillance, and other purposes. Some have even suggested that individual health care is so important that it should be the *only* purpose for which information can ever be used. These suggestions make it clear that the individual health care benefits of the NHIN must be the top priority of developers, and must be the centerpiece of public education programs. Individuals are typically willing to disclose information and absorb some risk to privacy if they get some direct personal benefit in return, but general improvements in quality assurance, outcomes research, decision support, and public health, or other diffuse societal benefits, are unlikely to persuade individuals to undertake the personal risk of making their own information health available over the NHIN. The focus of the NHIN developers and any public education efforts must be on direct, individual benefits and improving individual care.

Second, meaningful input and participation will help improve understanding of the system and increase the public's level of comfort that the NHIN's benefits outweigh its risks. We have previously indicated the importance of public participation in the design, functioning, and oversight of the NHIN. We also stressed the importance of carefully crafted regulatory procedures and enforcement authority. These "substantive" measures will help to instill public confidence in the operation of the system. In addition, AHIC and other groups should take special care in ensuring that the public is thoroughly and thoughtfully engaged in the development and oversight of the NHIN.

Third, HHS must establish an ongoing program of measuring and assessing the effectiveness of the privacy and confidentiality protections of the NHIN and the level of individual understanding and public confidence in those protections. The NCVHS believes that the NHIN will have greater credibility, and public trust will be enhanced if this research, at least initially, is undertaken by independent investigators who are contractors or grantees of HHS than if the review is performed internally by HHS.

Recommendations

R-24 Public and professional education should be a top priority for HHS and all other entities of the NHIN.

R-25 Meaningful numbers of consumers should be appointed to serve on all national, regional, and local boards governing the NHIN.

R-26 HHS should establish and support ongoing research to assess the effectiveness and public confidence in the privacy, confidentiality, and security of the NHIN and its components.

Post-Hearing Questions for the Record
Dr. Robert Kolodner
Interim National Coordinator for Health Information Technology
Department of Health and Human Services

"Private Health Records: Privacy Implications of the Federal Government's Health Information Technology Initiative"

February 1, 2007

Questions from Senator Daniel K. Akaka, Chairman

1. **You testified that there are differences between federal and state laws and that these differences provide additional challenges for sharing of health information in a private and secure manner. Can you elaborate on these challenges and how differences in federal and state laws are currently addressed in sharing paper-based health information?**

The promulgation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules established a federal floor of national standards to protect the privacy of individuals' health information, and at the same time allowed for more stringent state privacy laws and practices to continue to operate. Indeed, many states have laws that provide greater privacy protections, particularly with respect to certain types of "sensitive" information and often by requiring patient consent for certain disclosures for which the HIPAA Privacy Rule does not require patient authorization. Additionally personally identifiable information, including most medical information, maintained by or on behalf of a federal agency are protected under The Privacy Act of 1974 (Privacy Act) and are protected according to the security controls outlined in the Federal Information Security Management Act.

As the nation expands its use of interoperable electronic health records, the variation in state privacy laws and organizational-level business practices may pose considerable challenges to sharing information across organizations whose patients receive care in more than one state, which could make it difficult to achieve improvements in health care quality and efficiency.

A great deal of health information today is maintained on paper and most clinical health information is siloed – that is, kept and managed by a single provider or entity. For larger health care entities that conduct business in multiple states, cumbersome and expensive ways to cope with the differences among state laws are often necessary. These solutions would not necessarily be scalable to a more widespread, nationwide ability to exchange information between patients and providers in different states. Compliance with appropriate federal and state laws may require complex legal and compliance advice

and burdensome administrative processes, including multiple forms and notices. This is a result of varying levels of state protections and health care being conducted across state lines, something which occurs with paper or electronic records. Given the authorizations required, patients must often personally acquire their information from many sources to bring together sufficient information to make decisions regarding their medical care, and for clinicians to make treatment decisions. Absent a patient's direct involvement, a comprehensive health record is often unavailable to guide clinical decisions. This issue becomes more apparent with electronic records because of the potential ease of the "technical" aspects of information flow across jurisdictions. Since the decision to go "above the floor" of the HIPAA laws (with more protective measures) is made at the State level, information exchange between providers in that State is typically not impeded. Challenges may exist, however, when providers in two different states need to exchange information electronically. In this case, there may be different state-level protections in place for specific data types. Some examples of these differences could include protections surrounding a specific type of data (like HIV/AIDS information), or varying requirements for patient authorization to disclose certain data.

HHS, through the Privacy and Security Solutions for Interoperable Health Information Exchange, is working with 34 states and territories to assess variations in organization-level business practices and underlying state laws that pose challenges to electronic health information exchange (HIE). By early summer, this contract will result in the development of recommended solutions and implementation plans to support the secure and protected exchange of electronic health information within these states and territories. Additionally, the State Alliance for e-Health, formed through a separate contract, is designed to encourage state and territorial leaders in health information technology to develop consensus solutions for interstate policies regarding the exchange of interoperable electronic health information.

2. **The Office of the National Coordinator has made progress on several initiatives to protect personal health information. What entity is responsible for integrating the outcomes of these various privacy-related activities?**

The Office of the National Coordinator for Health Information Technology (ONC) is responsible for the integration of the various health IT privacy and security activities upon which HHS has embarked. This includes the development of privacy and security policies related to the adoption and use of interoperable health information technologies. Of course, to the extent that policies implicate other Departmental programs, ONC is coordinating such policy with the responsible components.

3. **According to Mr. Rothstein on our second panel, the four contractors selected by the Department of Health and Human Services to develop proposals for the national health information network architecture have not been required nor encouraged to include new privacy enhancing technologies, such as contextual access criteria. What privacy guidelines and directives were included in the contracts to develop the national health information architecture and why did the contracts fail to encourage the use of privacy enhancing technologies?**

The Nationwide Health Information Network (NHIN) vendors were required to develop security models in the prototype architectures and to work with their clinical consortia on security and confidentiality architecture challenges. These security models, in fact, included privacy-enhancing technologies in many important areas, such as the area of "consumer capabilities." These include capabilities for consumers to control access to their personal health record and to determine where their personal health records are managed. Also included in these capabilities are mechanisms by which consumers can indicate whether they want to participate in health information exchange and for that choice to be shared among network participants.

The security models and consumer capabilities developed in the 2006 NHIN work will be used to guide the 2007 NHIN work on trial implementations and to ensure that the NHIN advances the consumer and security capabilities to protect consumer interests.

ONC will also continue to work aggressively both through the follow-on NHIN Trial Implementations and with the Confidentiality, Privacy, and Security workgroup of the American Health Information Community to develop privacy and security policies to support the secure exchange of health information necessary to improve both the quality and efficiency of American healthcare.

Question from Senator George V. Voinovich, Ranking Member

1. **The Department of Health and Human Services has been criticized for not acting on the June 2006 recommendations made by the National Committee on Vital and Health Statistics. Would you please elaborate on how HHS has responded to the recommendations and identify what may be slowing action?**

HHS has an active interest in and has already begun to address the National Committee on Vital and Health Statistics (NCVHS) recommendations from the Privacy and Confidentiality in the Nationwide Health Information Network report to the Secretary in June 2006. After testimony extending 18 months, the NCVHS developed this letter-report, which included 26 recommendations on privacy and security policies for the Nationwide Health Information Network (NHIN). While a number of NCVHS recommendations offer precise advice, several reflected the Committee's reluctance to take a position on more contentious issues, such as a national policy on whether a consumer's choice to participate in the NHIN should be "opt-in" or "opt-out."

To that end, HHS, together with its advisory committees, is reviewing the recommendations to determine what additional knowledge is needed to arrive at more informed policies. The AHIC's Confidentiality, Privacy, and Security (CPS) workgroup and NCVHS's Privacy and Confidentiality subcommittee are each carving out an area for further inquiry identified by the recommendations. Specifically, the AHIC CPS has begun considering the implications of participants in electronic health information exchange (that are not subject to existing federal privacy and security requirements e.g., non-covered health care providers, personal health record vendors, and health

information exchanges) having the same access to personal health information as others who are subject to these laws.

In its April hearing, NCVHS will begin investigating the desirability and feasibility of allowing individuals to control access to the specific content of their health records via the NHIN and, if implemented, what limits might be appropriate. HHS staff are working closely with both groups. In addition, HHS will use the NCVHS recommendations to inform future contracts including the next round of the NHIN – "Trial Implementations." As we receive more information from various HHS activities such as the Privacy and Security Solutions for Interoperable Health Information Exchange contract with 34 states and territories and the State Alliance for e-Health, HHS will evaluate these inputs along with NCVHS and AHIC recommendations to determine the most appropriate mechanisms for action.

Post-Hearing Questions for the Record
Mr. Daniel Green
Deputy Associate Director, Center for Employee and Family Support Policy
Office of Personnel Management

"Private Health Records: Privacy Implications of the Federal Government's Health Information Technology Initiative"
February 1, 2007

Questions from Senator Daniel K. Akaka, Chairman

1. **What percentage of Federal Employee Health Benefit Program (FEHBP) plans use health IT? In what ways are those programs using health IT? For those programs not using health IT, what is the barrier for them to do so?**

   Virtually all FEHB plans are using health information technology in some form today. While we do not have exact percentages, most use electronic scanning and processing of claims; many are providing secure website access to personal health records (PHR) based on member claims information; and some are working with their contracted pharmacy benefits managers on ePrescribing.

   We have encouraged FEHB plans to offer PHRs to their members. The majority of plans are working toward a "web portal" that essentially connects members to their health plan website where they can access a variety of account functions, in addition to their PHRs. These include ordering ID cards, locating providers by zip code or other data, determining the status of their health benefits claim, etc. They can also use the website to obtain information on their benefits and preventive health and wellness information.

   Some plans have exhibited strong health IT leadership. Kaiser has a fully integrated electronic health record (EHR) underway for its health maintenance organization membership and is piloting a program whereby members can consult with their primary care providers through email. Some other plans are moving toward complex systems that deliver a variety of integrated uses, including personal health records (PHR), EMRs, electronic imaging for remote viewing, laboratory data integration and using captured health information for predictive modeling systems.

   In addition, health insurance industry leaders such as America's Health Insurance Plan (AHIP) and Blue Cross and Blue Shield Association (BCBSA) are working on identifying relevant data elements for PHRs and technical specifications for security and transferability of records from health plan to health plan when members elect to change plans during Open Season.
   While there is a lot of effort directed toward PHRs, EMRs and other uses for health information technology, there is much to be done. Issues such as privacy

and security of personal health information are critical to consumer acceptance of the Administration's health information technology initiatives. Other issues, such as standardized definitions for data, technical specifications for medical registries and prescription summaries, and the standards for interoperability of records among medical providers, hospitals, health plans, consumers, are still being developed and will need to be beta tested and certified by a reliable organization(s) in order to gain public acceptance. The Department of Health and Human Services is driving this monumental task forward and is working to ensure the process is a collaborative one and incorporates both public and private interests in identifying issues and coming to reasonable solutions.

2. **According to a May 15, 2006, Federal Times article entitled, "Your health records online," (http://www.federaltimes.com/index.php?S=1771146) as soon as 2009 the Office of Personnel Management (OPM) will begin cutting profits for plans that are slow to adopt health IT by lowering the premiums they can charge enrollees. Given the fact that the Department of Health and Human Services (HHS) still has not developed the nation-wide infrastructure for the sharing of health information nor has it address the privacy implications of the electronic sharing of health information, is OPM still planning to cut the profits for FEHBP plans by 2009?**

   In July 2004, OPM issued a report to the President in response to Executive Order 13335, *Incentives for the Use of Health Information Technology*. In the report, OPM expressed willingness to explore various options to speed the nationwide phase-in of health information technology as soon as practicable. One of the options was to strongly encourage Federal Employees Health Benefits (FEHB) Program carriers to adopt health information technology by providing incentives for ePrescribing and contracting with providers which use electronic medical records. We have advised carriers that adoption of HIT would become an element of our plan performance review within the next two to four years.

   We are working with the Department of Health and Human Services (HHS) and other Federal agencies on adoption of recognized health information technology interoperability standards so that patient health information can be shared securely and seamlessly. OPM has started working on language for its 2008 FEHB carrier contracts to reflect the requirements of the Executive Order. At the same time, we want to ensure that FEHB carriers are adopting standards as they are simultaneously being adopted and implemented by others in the healthcare industry. As OPM implements health information technology initiatives, we will determine how best to measure plan performance and profit.

Question from Senator George V. Voinovich, Ranking Member

How does OPM see what is being done through the Federal Employees Health Benefits Program impacting health information technology throughout the country?

On August 22, 2006, President Bush signed an executive order committing Federal healthcare programs to four "cornerstone" goals. Health and Human Services Secretary Michael Leavitt has called on all employers to commit to the four "cornerstones" and to take a leadership role in value-based healthcare purchasing.

The FEHB Program is often viewed as a model employer-sponsored health benefits program that serves as a barometer within the healthcare industry. We have advised all FEHB carriers that we expect them to demonstrate their commitment to the four "cornerstones" which means:

1. Using recognized HIT interoperability standards so that patient health information can be shared securely and seamlessly;
2. Reporting on quality of care, so that consumers and providers can learn how well each provider measures up in delivering care;
3. Providing transparency on costs of health services so that consumers can make better healthcare decisions on quality and the costs they will pay; and,
4. Providing insurance options that reward consumers for the choices they make based on quality and cost.

We believe the Federal Government and America's employers, working alongside health insurance plans and providers, can help bring about uniform approaches to value-based purchasing which can contribute to information consumers use to make informed health choices.

United States Government Accountability Office
Washington, DC 20548

March 14, 2007

Senator George V. Voinovich
Ranking Member
Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia
Committee on Homeland Security and Governmental Affairs
United States Senate

Subject: *Private Health Records: Privacy Implications of the Federal Government's Health Information Technology Initiative*

Dear Senator Voinovich:

This letter responds to your request that we answer a question relating to our testimony of February 1, 2007.[1] In that testimony, we discussed steps the Department of Health and Human Services (HHS) is taking to ensure privacy protection as part of its national health information technology strategy. Your question, along with our response, follows.

1. *Entities such as the American Health Information Community and the National Committee on Vital and Health Statistics offer recommendations to the Secretary of Health and Human Services on implementation of health information technology. Do you believe the Office of the National Coordinator has sufficient authority to facilitate communication among federal entities, the private sector, and consumer organizations to lead the development and implementation of appropriate privacy standards?*

The Office of the National Coordinator has authority to facilitate coordination and communication among the many stakeholders in the nation's health care industry. In April 2004, President Bush issued an executive order that gave the National Coordinator authority to coordinate and facilitate communication among federal entities, the private sector, and consumer organizations on all HHS health information technology policies and programs.[2] However, the office's ability to effectively lead efforts to define and implement appropriate health information privacy standards is hindered by its lack of an overall approach for protecting electronic health information. As we stated in our testimony on February 1st, such an

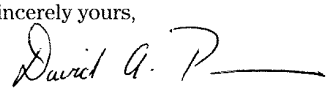
[1] GAO, *Health Information Technology: Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy*, GAO-07-400T (Washington, D.C., February 1, 2007)
[2] Executive Order 13335, *Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator* (Washington, D.C., Apr. 27, 2004)

approach is needed to identify milestones for integrating and implementing the outcomes of the Office of the National Coordinator's various privacy-related initiatives, including defining and implementing standards. An overall privacy approach is also needed to ensure that key privacy principles are identified and fully addressed. Without such an approach, it will be difficult for the Office of the National Coordinator to effectively facilitate coordination and communication among federal, private industry, and consumer stakeholders that lead to the definition and implementation of adequate privacy standards for a nationwide health information network.

In responding to this question, we relied on our prior work on HHS's initiatives that are intended to address the privacy and security of health information exchanged within a nationwide health information network. We performed our prior work in accordance with generally accepted government auditing standards.

Should you or your office have any questions on matters discussed in this letter, please contact me at (202) 512-9286 or pownerd@gao.gov.

Sincerely yours,



David A. Powner
Director, Information Technology
Management Issues