AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

PROTECTING PATIENT PRIVACY IN HEALTHCARE INFORMATION SYSTEMS

HEARING

BEFORE THE

SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

JUNE 19, 2007

Serial No. 110–33

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html
http://www.oversight.house.gov

U.S. GOVERNMENT PRINTING OFFICE

39–023 PDF WASHINGTON : 2008

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

COMMITTEE ON OVERSISGHT AND GOVERNMENT REFORM

HENRY A. WAXMAN, California, *Chairman*

TOM LANTOS, California
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
BRIAN HIGGINS, New York
JOHN A. YARMUTH, Kentucky
BRUCE L. BRALEY, Iowa
ELEANOR HOLMES NORTON, District of Columbia
BETTY McCOLLUM, Minnesota
JIM COOPER, Tennessee
CHRIS VAN HOLLEN, Maryland
PAUL W. HODES, New Hampshire
CHRISTOPHER S. MURPHY, Connecticut
JOHN P. SARBANES, Maryland
PETER WELCH, Vermont

TOM DAVIS, Virginia
DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
JOHN M. McHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
JOHN J. DUNCAN, JR., Tennessee
MICHAEL R. TURNER, Ohio
DARRELL E. ISSA, California
KENNY MARCHANT, Texas
LYNN A. WESTMORELAND, Georgia
PATRICK T. McHENRY, North Carolina
VIRGINIA FOXX, North Carolina
BRIAN P. BILBRAY, California
BILL SALI, Idaho
JIM JORDAN, Ohio

PHIL SCHILIRO, *Chief of Staff*
PHIL BARNETT, *Staff Director*
EARLEY GREEN, *Chief Clerk*
DAVID MARIN, *Minority Staff Director*

SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES

WM. LACY CLAY, Missouri, *Chairman*

PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
JOHN A. YARMUTH, Kentucky
PAUL W. HODES, New Hampshire

MICHAEL R. TURNER, Ohio
CHRIS CANNON, Utah
BILL SALI, Idaho

TONY HAYWOOD, *Staff Director*

CONTENTS

PROTECTING PATIENT PRIVACY IN HEALTHCARE INFORMATION SYSTEMS

TUESDAY, JUNE 19, 2007

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 2 p.m. in room 2154, Rayburn House Office Building, Hon. Wm. Lacy Clay (chairman of the subcommittee) presiding.

Present: Representatives Clay, Maloney, Hodes, and Turner.

Staff present: Tony Haywood, staff director/counsel; Jean Gosa, clerk; Adam C. Bordes, professional staff member; Nidia Salazar, staff assistant; Charles Phillips, minority counsel; Allyson Blandford, minority professional staff member; Patrick Lyden, minority parliamentarian and member services coordinator; and Benjamin Chance, minority clerk.

Mr. CLAY. The Subcommittee on Information Policy, Census, and National Archives will come to order.

Let me begin by saying good afternoon and welcome to today's hearing on efforts to protect the privacy of personal health information in electronic health care information systems.

The use of IT to store, share, and secure electronic health information has expanded rapidly in recent years. Many insurers and hospitals have already transitioned from paper-based records to electronic medical record systems for exchanging patient data. This has brought important benefits to both patients and providers, including shorter hospital stays, improved management of chronic disease, and fewer redundant tests and examinations.

Americans have expressed legitimate concerns, however, about the potential for improper disclosure of personally identifiable health care information. Before they will fully embrace the benefits and efficiencies of e-health solutions, patients must be confident that personal information in electronic format is as secure and private as information in paper records.

A nationwide health information network promises tremendous benefits for patients. For 3 years the Department of Health and Human Services has been working to make the idea technically and economically feasible. Unfortunately, a January 2007 GAO report found that HHS was not doing enough to integrate effective privacy safeguards into its long-term national strategy for health IT. Varying health IT privacy standards in different States are another area of concern.

While the enactment of the Health Insurance Portability and Accountability Act [HIPAA], in 1996 was an important step forward, it has left patients with disparate privacy protections. I believe we should amend HIPAA to extend the most effective and practical privacy safeguards to everyone.

I introduced bipartisan legislation in the 109th Congress which proposed to establish a framework for a uniform national health privacy standard. Giving patients greater personal control over their health information is critical; therefore, putting in place stricter notice and consent requirements for all third-party disclosures and information sharing activities is an important legislative objective for Congress to achieve.

Today's hearing will allow different perspectives on these issues to be aired as we move toward implementing a national health care information network.

I must say that I am disappointed that HHS was unable to supply a suitable witness to appear today on behalf of the administration, but the Department has submitted written testimony for today's hearing, and I will ask GAO and our other witnesses to respond to positions stated in that testimony.

I look forward to the testimony of all of our witnesses.

[The prepared statement of Hon. Wm. Lacy Clay follows:]

Opening Statement of Rep. Wm. Lacy Clay (D-MO), Chairman
Subcommittee on Information Policy, Census, and National Archives
House Committee on Oversight and Government Reform

Hearing on "Protecting Patient Privacy in Healthcare Information Systems"

June 19, 2007

Good afternoon and welcome to today's hearing on efforts to protect the privacy of personal health information in electronic healthcare information systems.

The use of information technology to store, share, and secure electronic health information has expanded rapidly in recent years. Many insurers and hospitals have already transitioned from paper-based records to electronic medical record systems for exchanging patient data. This has brought important benefits to both patients and providers, including shorter hospital stays, improved management of chronic disease, and fewer redundant tests and examinations.

Americans have legitimate concerns, however, about the potential for improper disclosure of personally identifiable healthcare information. Before they will fully embrace the benefits and efficiencies of e-health solutions, patients must be confident that personal information in electronic format is as secure and private as information in paper records.

A nationwide health information network promises tremendous benefits for patients. For three years, the Department of Health and Human Services has been working to make the idea technically and economically feasible. Unfortunately, a January 2007 GAO report found that HHS was not doing enough to integrate effective privacy safeguards into its long-term national strategy for health I.T. We'll discuss GAO's report this afternoon.

Varying health IT privacy standards in different states are another area of concern. Enacted in 1996, the Health Insurance Portability and Accountability Act, or HIPAA, established baseline national standards to protect the privacy of personal health information. This was an important step forward, but it leaves patients in different states with disparate privacy protections. I believe we should amend HIPAA to extend the most effective and practical privacy safeguards to everyone. Bipartisan legislation that I introduced in the 109th Congress proposed to do that by establishing a framework for a uniform national health privacy standard.

Giving patients greater personal control over their health information is also critical. Therefore, putting in place stricter notice and consent requirements for all third party disclosures and information-sharing activities is an important legislative objective for Congress to achieve.

Today's hearing will allow different perspectives on these issues to be aired as we move toward implementing a national healthcare information network. I must say that I am deeply disappointed that HHS was unable to supply a suitable witness to appear today on behalf of the Administration; but the Department has submitted written testimony for today's hearing, and I'll ask GAO and our other witnesses to respond to positions stated in that testimony. I look forward to the testimony of all of our witnesses.

Mr. CLAY. I assume when the ranking member gets here he will have an opening statement and we will yield to him for that, but for now we will proceed with the hearing.

If we don't have any additional statements, the subcommittee will now hear testimony from the witnesses before us today.

On our first panel we will hear from Valerie C. Melvin, Director for Human Capital and Management Information Systems Issues at GAO. Welcome, Ms. Melvin.

Accompanying Ms. Melvin is Linda D. Koontz, Director for Information Management Issues at GAO. Welcome to you.

Ms. Melvin will deliver GAO's formal testimony, and both will respond to questions.

Thank you for appearing before the committee today. It is the policy of the Committee on Oversight and Government Reform to swear in all witnesses before they testify. Will you both please stand and raise your right hands?

[Witnesses sworn.]

Mr. CLAY. Let the record reflect that the witnesses answered in the affirmative.

Ms. Melvin, you will have 5 minutes to make an opening statement. Your complete written testimony will be included in the hearing record.

The lighting system and the timing system does not work, so we will notify you probably through the use of the gavel when you get close to the 5-minute time limit.

Mr. Turner, thank you for being here.

Mr. TURNER. Mr. Chairman, thank you.

Mr. CLAY. OK. And you may, if you have an opening statement, you may proceed, sir.

Mr. TURNER. Thank you, Mr. Chairman. I appreciate that and I apologize for my being late.

I want to thank you for holding this important hearing on privacy concerns and health information technology. Many health care experts agree that investing in health information technology will dramatically improve patient care while simultaneously decreasing health care costs.

For example, Kettering Medical Center in my District and its partners have created the Dayton Individual Health Record Pilot Project, IHR. The Dayton IHR pilot combines a patient's health information from different sources and presents that information to patients, doctors, and other health care professionals in a format that helps all health participants make efficient, appropriate decisions about their care options.

The Dayton IHR is a Web-based record that allows a patient to access their information from their home, the office, or even if the patient ends up in an emergency room in another town.

While it is important that technology like the Dayton IHR be made available, it should not be available at the sacrifice of patient privacy and security. The Dayton IHR ensures that only the patient and the physicians granted access by the patient can look at the information within the IHR.

This subcommittee has previously discussed privacy concerns in relation to Federal IT infrastructures, and I expressed my concerns

with how IT breaches affect individuals, as well as national security.

Health care raises unique privacy concerns, but I am interested to learn how we can work with all stakeholders to address important privacy issues and facilitate the adoption of health IT. Health IT holds the promise of increasing the quality of health care, as well as decreasing health care costs for American families. We must be careful, however, to reach these goals without sacrificing the security of professional health information.

I look forward to hearing the information from today's witnesses on this important topic, and I yield back the remainder of my time.

Thank you.

Mr. CLAY. Thank you so much, Mr. Turner.

We will begin with Ms. Melvin.

You may proceed.

STATEMENT OF VALERIE C. MELVIN, DIRECTOR OF INFORMATION MANAGEMENT ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE, ACCOMPANIED BY LINDA D. KOONTZ, DIRECTOR FOR INFORMATION MANAGEMENT ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

Ms. MELVIN. Thank you, Mr. Chairman and Ranking Member Turner.

We are pleased to be here today to testify on privacy issues associated with efforts to increase the use of information technology in the health care industry. As noted, with me today is Linda Koontz, Director of Information Management Issues, who is responsible for GAO's privacy work.

In 2004 President Bush issued an Executive order that called for widespread adoption of interoperable electronic health records by 2014 and established a National Coordinator for Health IT to lead and foster public/private coordination.

The benefits of health IT are immense, and include reducing medical errors and improving public health emergency response. However, the increasing use of technology also raises concerns regarding the extent to which patient privacy is protected. The challenge is to strike the right balance between patient privacy concerns and the numerous benefits that IT has to offer.

Over the past few years, we have issued reports and testified numerous times on HHS' efforts toward defining a national health IT strategy. Among these reports, one issued last January highlighted HHS' health IT privacy initiatives. Today, as requested, I will summarize the results of that study, highlighting three points: the importance of having a comprehensive privacy approach, HHS' initial efforts to address privacy as part of its national health IT strategy, and additional efforts needed.

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 with the transition to using more electronic health records. A comprehensive privacy approach is needed to determine how personally identifiable information will be disclosed, used, and protected.

HHS acknowledges in its national health IT framework the need to protect consumer privacy, and it plans to develop and implement privacy and security policies, practices, and standards for electronic health information exchange. To this end, HHS and its Office of the National Coordinator have initiated several efforts, including awarding contracts, including 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.

Ultimately, the National Coordinator's Office intends to use the results of these initiatives to identify policy and technical solutions for protecting personal health information as part of its continuing efforts to complete a national health IT strategy. However, while these efforts are good building blocks on which progress has been made, important work remains, including assessing how variations in State laws affect health information exchange, acting on the privacy and security contractor's findings and advisory group recommendations, and identifying and implementing privacy and security standards.

Moreover, how and when HHS plans to integrate the outcomes of these initiatives is unclear; thus, we have recommended that HHS develop an overall privacy approach that identifies milestones in an accountable entity for integrating the outcomes of its health IT contracts and advisory group recommendations, ensures that key privacy principles are fully addresses, and addresses key challenges associated with legal and policy issues and the disclosure, access to, and security of information.

In recent discussions with us, the National Coordinator committed to developing a plan that would accomplish these objectives. In this regard, he announced last weekend an initiative to build consensus around a harmonized set of privacy and security principles which are to serve as a framework for addressing these important issues.

Overall, Mr. Chairman, the National Coordinator's intent to act on such an approach is promising, and building a framework based on fair information principles is a good starting point for moving forward; however, achieving this goal to safeguard personal health information will be difficult and plagued with challenges and will necessitate sustained leadership from HHS to realize success.

This concludes our prepared statement. We would be pleased to respond to any questions that you may have.

[The prepared statement of Ms. Melvin follows:]

United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Information Policy, Census, and National Archives Committee on Oversight and Government Reform
U.S. House of Representatives

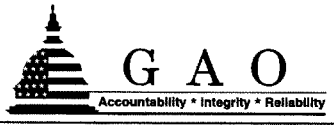
For Release on Delivery
Expected at 2:00 p.m. EDT
Tuesday, June 19, 2007

HEALTH INFORMATION TECHNOLOGY

Efforts Continue but Comprehensive Privacy Approach Needed for National Strategy

Statement of
Linda D. Koontz
Director, Information Management Issues

Valerie C. Melvin
Director, Human Capital and Management Information Systems Issues



GAO-07-988T

June 19, 2007

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-988T, a testimony before the House Subcommittee on Information Policy, Census, and National Archives; Committee on Oversight and Government Reform

HEALTH INFORMATION TECHNOLOGY

Efforts Continue 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 information technology (IT). The plan is to recommend methods to ensure the privacy of electronic health information.

GAO was asked to summarize its January 2007 report. 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 initial comments, HHS disagreed with this recommendation and stated that it had established a comprehensive privacy approach. In recent discussions with GAO, the National Coordinator for Health IT agreed with the need for an overall approach to protect health information and stated that the department was initiating steps to address the recommendation.

www.gao.gov/cgi-bin/getrpt?GAO-07-988T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Valerie C. Melvin, (202) 512-6304, melvinv@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. HHS's 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. 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 its 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 and 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 (HIPAA) 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.

At your request, our testimony today summarizes our January 2007 report 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] The testimony also describes relevant activities that HHS

[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).; GAO, *Health Information Technology: Early Efforts Initiated, but Comprehensive Privacy Approach Needed for National Strategy*; GAO-07-400T (Washington, D.C.: Feb 1, 2007)

has reported undertaking since our January report. In preparing for this testimony, we relied primarily on our work supporting the report, which contains a detailed overview of our scope and methodology. The work on which this testimony is based 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 (NCVHS) 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 recommended 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 commenting on 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."

While we acknowledged in our report that HHS had initiated key efforts to address its objective to protect consumer privacy, we found that HHS's approach for addressing privacy and security did not address elements that should be included in a comprehensive privacy approach, such as milestones for integration, identification of the entity responsible for integrating the outcomes of privacy-related initiatives, and plans to address key privacy principles and challenges. In recent discussions with GAO, the National Coordinator for Health IT agreed with the need for an overall approach to protect health information and stated that the department was initiating steps to address our recommendation.

Further, since our report was issued, HHS reported that it has undertaken additional activities to address privacy and security concerns. For example, NCVHS's subcommittee on privacy and confidentiality has drafted additional recommendations to the Secretary of HHS regarding the expansion of health information privacy law coverage to entities that are not currently covered. In addition, the privacy and security solutions contractor is in the process of analyzing 34 states' final assessments of organization-level business practices. Also, HHS has awarded a new contract, the State Alliance for e-Health, which is intended to identify state-level health IT issues, including challenges to ensuring the privacy of health information and solutions for providing security.

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

[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-04-917T (Washington, D.C.: July 14, 2004).

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 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 HIPAA. This law provided for the Secretary of HHS to establish the first broadly applicable federal privacy and security measures 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

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

[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 ensure that such information is reasonably and appropriately safeguarded. 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

[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.

ensure that covered entities have proper security controls in place 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 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. In January 2007, the work group presented recommendations on performing patient identity proofing to AHIC. The recommendations were approved by AHIC and submitted to HHS. 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 over 80 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 nationwide 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 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 recommended 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, in recent discussions with GAO, the National Coordinator

[14]GAO-07-238.

for Health IT agreed with the need for an overall approach to protect health information and stated that the department was initiating steps to address our recommendation.

Further, since our report was issued, HHS has reported that it has undertaken additional activities to address privacy and security concerns. For example:

- NCVHS's subcommittee on privacy and confidentiality is drafting additional recommendations for the Secretary of HHS regarding the expansion of the HIPAA Privacy Rule coverage to entities that are not currently covered. The recommendations are expected to be presented to the NCVHS at its meeting later this month.
- The privacy and security solutions contractor is in the process of analyzing and summarizing 34 states' final assessments of organization-level business practices and summaries of critical observations and key issues. Its initial assessment identified challenges that closely parallel those identified in our report. HHS plans to finalize the findings and final reports from the contractor after the contract ends at the end of this month.
- HHS awarded another contract, the State Alliance for e-Health, which is intended to address state-level health IT issues, including privacy and security challenges and solutions. In January 2007, the alliance identified the protection of health information as a guiding principle for its work. The alliance plans to identify privacy practices and policies to help ensure the protection of personal health information exchanged within a nationwide health information network.

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 has 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 remains highly 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. If implemented properly, HHS's planned actions could help improve efforts to address key privacy principles and the related challenges, and ensure that the department meets its goal to safeguard personal health information as part of its national strategy for health IT.

Mr. Chairman and members of the subcommittee, this concludes our statement. We would be happy to respond to 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 D. Koontz at (202) 512-6240 or Valerie C. Melvin at (202) 512-6304 or by e-mail at koontzl@gao.gov or melvinv@gao.gov. Other key contributors to this testimony include Amanda C. Gill, Nancy E. Glover, M. Saad Khan, David F. Plocher, and Teresa F. Tucker.

GAO's Mission	The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."
Order by Mail or Phone	The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to: U.S. Government Accountability Office 441 G Street NW, Room LM Washington, D.C. 20548 To order by Phone: Voice: (202) 512-6000 TDD: (202) 512-2537 Fax: (202) 512-6061
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Web site: www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400 U.S. Government Accountability Office, 441 G Street NW, Room 7125 Washington, D.C. 20548
Public Affairs	Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, D.C. 20548

PRINTED ON RECYCLED PAPER

Mr. CLAY. Thank you so much, Ms. Melvin.

According to their written testimony, HHS states that it has invested significant resources and efforts in our nationwide strategy for protecting health information. Our national health IT agenda approaches our privacy and security through a full suite of activities both in form of current work and preparing for future needs. Specifically, HHS mentions authorizing a review of 34 States and Puerto Rico to analyze how their laws are affecting the sharing of health information. Yet, GAO's January 2007 report cites HHS' lack of an overall strategic plan for integrating its privacy initiative into a health information network. The report also concludes that HHS lacks appropriate milestones to measure its progress to meet these requirements.

With that in mind, I would like to ask the following question: can you explain how HHS is addressing the legal barriers associated with variances in State privacy laws and methods to limit the types of information disclosed through a nationwide exchange? And is it true that HHS disagrees with GAO's recommendation to establish milestones to measure progress and outcomes in the development of privacy protections for a network? If so, why?

Ms. MELVIN. When our report was issued, our concern was that HHS did not have, as you said, an integrated plan that would allow all the various initiatives that it has undertaken to be integrated and to be guided by milestones and measure its progress, and also from the standpoint of having a leader to make sure that there would be complete integration of the various initiatives to guide the overall effort.

There are other factors related to the variations in the State agencies. They do, in fact, have contracts in place that are intended to assess those, as you have mentioned, and those types of initiatives are all the ones that we believe have to be guided and driven by an overall integrated plan that has a well-defined approach to bringing together the specific initiatives, to being able to look at all of the findings and the assessments that are being made, and to develop and implement solutions as a result of what their assessments have determined.

Mr. CLAY. Well, can you identify for us the entity or entities within HHS that will be responsible for coordinating and implementing its privacy initiatives? Who will promulgate the regulations and oversight activities for privacy within the network? Is this entity effectively staffed and capable of managing its responsibilities?

Ms. MELVIN. One of the key areas or pieces of information that we believe is missing is the identification of the critical entity that would be responsible for bringing together all of the initiatives, as you have noted, so we cannot identify at this time who that would be. We do understand, through our recent discussions with Dr. Kolodner, that the agency is taking steps through the National Coordinator's Office to implement a framework; however, how that framework will be put in place and who will actually guide and lead their efforts to accomplish that has not been specified and we have no information that we could share regarding its——

Mr. CLAY. They don't know yet? I mean, you gave them that report in January of this year.

Ms. MELVIN. Yes.

Mr. CLAY. And they have not moved on the recommendations is what you are telling me?

Ms. MELVIN. As of last week when we spoke with Dr. Kolodner their efforts were in the early stages and there was no specific information provided to us relative to who the entity would be that would lead all of those efforts.

I should note that when our report was issued the National Coordinator's Office did have a difference relative to how they should proceed with a coordinated approach, so it has only been in recent times that we have now, I think, reached more agreement with them relative to the importance of having a plan in place, an approach that would, in fact, include and identify a specific leader for integrating or overseeing the integration of the various initiatives.

Mr. CLAY. Thank you for that. And this is a question for either one of you. One of HIPAA's limitations is that it does not cover all entities that possess or utilize personal health information. Some life insurers and research entities that are not involved with the treatment of patients fall outside the rules. Have you examined the practical impact of not covering some entities that have access to personal health information? Is this a significant problem, in your view, Ms. Koontz?

Ms. KOONTZ. I think that is a significant issue that deserves more study, and we would like to see HHS consider that as it moves forward in developing privacy policies, practices, and standards. It is true that HIPAA covers health plans, health providers who transmit electronic information in support of transactions, and health information clearinghouses. The entities that you mentioned are outside the coverage of HIPAA. I think that, naturally, as we move to a national health information network in which it will be much easier, and it is actually intended to make information flow more easily, this is something that we should pay a lot more attention to. Again, I do hope that HHS includes this in their deliberations as they move forward.

Mr. CLAY. OK. Thank you for your response.

Let me now turn to my ranking member, Mr. Turner.

You may proceed.

Mr. TURNER. Thank you.

Thank you for the information you have provided to us in your testimony today. This is an important issue on pretty much three fronts. We have our desire to find cost savings and reduce the spiraling increases in health care costs. The second issue is quality of health care. What can we do to increase the quality of health care? And the third issue is: how do you balance privacy?

So many times when we make an advance in one area privacy either takes a hit, or when we think we are taking an advance in privacy others take a hit.

I will tell you one funny story. Two years ago when I was in Washington I broke my sunglasses. I called my wife at home and said, can you go and get me some new sunglasses. I have a prescription. She goes to the eyeglass place and they wouldn't let her buy eyeglasses because they said under HIPAA there is a fear that she would discover what my prescription is. You know, that is not exactly something that I have a concern about having a privacy ex-

pectation. But, nevertheless, that was the application. We had to wait until I returned back home until I could get them.

So this is a fine balance of what things do we have an expectation of privacy, and what things are important for efficiency, and what things do we have for cost savings, and many times there are unintended consequences—you know, I can't get my sunglasses unless I am back home—that are overlooked. What confidence do you have, in describing the process that we are undertaking, that the Federal Government is going to be able to have a better record in ascertaining that yes, we really need to protect people's privacy, yes, we need to find cost savings, and we need to find efficiencies to increase quality of health care? What are your thoughts?

Ms. MELVIN. Again, I think the confidence will grow from the extent to which there is transparency in the way that the health information network is put together and the way that privacy is conveyed to and understood by the public.

Our work has emphasized the need for the National Coordinator's Office and HHS to spend significant time in making sure that there is outreach and consensus to bring together a better understanding among all participants that would be involved in the overall health initiative.

You are right, there is an extremely fine balance between the privacy issues and the need to ensure quality care, the need to try to have improvements in the way that information is made available about care, and all of that comes through, again, having a defined plan for how they will do that, as well as having necessary outreach, necessary information made available to educate the public on the need for and the use of electronic health records so that certainly at some point hopefully there would be buy-in, more buy-in to make this a more successful effort.

So I think overall success will depend on how well they can really communicate and convey the need for and ultimately to implement a system that does balance privacy and security with the quality of the care that is being provided.

Mr. TURNER. One of the issues that has been identified is the cost savings that we expect from going to electronic recordkeeping, and the implementation of technology on this issue is that we don't really know what our cost savings would be, and we are not capturing in a very effective way how this might advance us in cost. Do you agree with that? And also, do you have thoughts as to what we could be doing better to understand really what will we be able to effect in cost savings in this?

Ms. MELVIN. I think clearly the cost savings is an issue. The overall cost of the initiative is an issue that would have to be defined based on what technology is ultimately determined to be needed and put in place for this, again largely driven by the privacy and policy security implications that would drive the technology that would need to be put in place.

Then ultimately, as a part of the overall strategy and the defined approach that the agency would need to have, a key part of that is defining what the costs are, what the outcomes that result from that are in the way of benefits and savings. I think all of those aspects collectively are going to be important in defining what the actual cost is ultimately for the overall initiative.

Mr. TURNER. Thank you, Mr. Chairman.

Mr. CLAY. Thank you, Mr. Turner.

We have been joined by our colleague from New Hampshire, Mr. Hodes.

I understand you have an opening statement. You may proceed with that and then go into your questions.

Mr. HODES. Thank you, Mr. Chairman.

Mr. CLAY. You have ample time. You are welcome.

Mr. HODES. This is a very important hearing. The privacy concerns related to health information technology in the digital age take on an increasingly important role as we examine a health care system which many people feel is a system which is dysfunctional and not operating as it should, and many are looking to electronic medical records technology as a key component to making our health care system a better-functioning system.

It seems that it is fairly obvious, at least to me, that there are great benefits in increased coordination of care from effective and appropriately constructed medical records technology systems, because instead of having people carrying around paper records and sacks of pills from one doctor to another and having the second doctor trying to figure out what it is that patient is on, we can quickly and easily, with medical records technology, determine what care that patient has had.

On the other hand, medical records technology presents great risks to patient security and private information. We have recently seen in the Veterans Administration, which frankly is in the forefront of developing electronic medical records technology, when a single laptop is lost there is enormous amounts of personal data that is compromised. So coming up with the right construct and the right system is clearly very important, and it is, I think, an urgent matter for us because there are a number of initiatives, both in the private sector and in Government, that are taking us down the road, but it sounds from your testimony and the report that there is still a very, very long way to go in coming up with an appropriate national system.

[The prepared statement of Hon. Paul W. Hodes follows:]

Congressman Paul Hodes
Opening Statement
Information Policy, Census, and National Archives Subcommittee
Oversight and Government Reform Committee
Tuesday, June 19, 2007
2154 Rayburn HOB – 2:00 P.M.
"Protecting Patient Privacy in Healthcare Information Systems"

Thank you Chairman Clay for holding this important hearing today on the privacy concerns related to health information technology. We live in a digital age. Increasingly, our medical records are no longer file folders on the walls of our doctors' offices, but bytes of information on hard drives and servers. Advances in technology and in electronic medical records make it easier for doctors to consult with other doctors and specialists, and allow insurance companies to efficiently communicate with providers. Health IT helps us determine the efficacy and efficiency of medical treatment, and saves lives by reducing medical errors.

With all the clear benefits that Health IT provides us, we need to make sure that personal health information is kept safe and secure. Careless practices and behaviors can lead to catastrophic results. When a Department of Veterans' Affairs employees lost ***one*** hard drive and ***one*** laptop, millions of

veterans' personal information was compromised. Losing a laptop is a lot easier than losing millions of file folders.

We need strong and clear laws to address the new vulnerabilities in health care privacy. HIPAA was enacted to address some of these digital privacy weaknesses. But, eleven years and many technological advances later, we need to revisit how health information privacy can be strengthened and secured.

It is imperative that we determine and implement the best practices to protect personal health information, both within the government and throughout the private sector. We need clear standards and robust laws to ensure that all those who handle our medical information do so with strong privacy and security safeguards in place.

I look forward to hearing from the panelists today on their recommendations to help us reap the benefits of Health IT in a way that also protects our privacy.

Mr. HODES. One question, Ms. Melvin, that I had raised by your testimony that I would just like you to clarify for me, if you could, would be—and I may not have all the terms right—but you mentioned that the National Coordinator's Office at HHS, I believe, had a difference about a national coordinated approach when your report was initially sent over?

Ms. MELVIN. We had originally recommended that they develop a defined approach that would, in fact, allow them to integrate the various initiatives, that would establish milestones and timeframes for the completion of initiatives, obviously considering that there were multiple activities going on, and that would, in fact, designate a leader, identify a leader who would lead the overall coordination, an entity that would lead the overall coordination of all of the various initiatives being put in place.

I believe that in this case in their comments HHS essentially believed that they did have a comprehensive approach. We had a difference relative to the construct of that approach and whether, in fact, it contained all of the necessary or recognized all of the necessary components in the way of having a designated leader, in the way of having established milestones, and potentially measures for being able to really gauge progress and to guide the overall effort.

Mr. HODES. And I gather there were some discussions that took place?

Ms. MELVIN. We have subsequently met with Dr. Kolodner, actually within the last week. We have talked more about what our concerns were relative to the lack of such a defined approach, and in talking with him and through information that we have seen since our discussions, there is an indication that he is in agreement with the need for having an approach, some type of road map that would, in fact, provide more detail than defined milestones for integrating the various initiatives that are underway.

Mr. HODES. There is no disagreement between you and Dr. Kolodner that the coordinator of any national health information technology system would be situated at HHS, is there?

Ms. MELVIN. We have not talked specifically about what entity would be the leader to integrate this. Our discussions were at a level relative to the importance, the significance overall of developing an approach. We have not described what that approach would be. We do feel it is important, however, that approach does, in fact, define those critical elements relative to timeframes and milestones, measures of performance, and also in terms of actually identifying the entity that would lead it, but we have not talked about specifically who that entity would be.

Mr. HODES. You are just trying to get to square one with HHS and have them recognize that there needs to be a coordinated approach with time lines and benchmarks and setting out a plan to put together the initiatives that have already been begun into some comprehensive plan that we can all look at and then talk about?

Ms. MELVIN. That is absolutely correct, sir.

Mr. HODES. I am just about finished, Mr. Chairman.

When you say that Dr. Kolodner has indicated his agreement, is that verbally? Is that in writing? How has that agreement been indicated?

Ms. MELVIN. Our discussions have been held through a meeting with Dr. Kolodner relative to what actions they were taking, but, as I stated earlier, we have not discussed the specifics of what that planned approach would look like ultimately. It is our hope, and we do view, you know, the fact that at this point he does agree with the need for that as very promising, but, as our statement indicates, it is a very difficult task. It is a long road. It does involve a lot of initiatives, and it will take sustained and committed effort on HHS' part to make sure that happens.

Mr. HODES. What is your timeframe for getting some sort of concrete response beyond the verbal discussions you have had from Dr. Kolodner and HHS that would clearly indicate, something we could look at, that says HHS agrees that we are going down this road and here is how we are going to get there? Are we talking a week? A month? Two months?

Ms. MELVIN. We have not specified a specific timeframe. Obviously, based on our recommendation, we do feel it is very important that this effort be undertaken urgently. It is very critical from the standpoint of the many initiatives that HHS and the National Coordinator's Office does have underway that lead to the development of technology, the significant point being that you want security and privacy policies to be in place to really guide and be a factor in determining what technology is there. So it is an urgent effort, but not one that we put a definite timeframe on for seeing that it happens.

Mr. HODES. Thank you very much.

Thank you, Mr. Chairman.

Mr. CLAY. Thank you, Mr. Hodes, for that line of questioning.

This question is for either/or. I would like to hear your thoughts on HHS' enforcement policies, practices, and procedures. There has been significant criticism of the agency's enforcement of HIPAA and lack of civil penalties enforced on identified violations. Are the enforcement activities of HHS being carried out in accordance with the statute and the legislation and regulations? Are the current regulations adequate to ensure that violating entities are being sanctioned appropriately?

Ms. KOONTZ. I have to say, first of all, that we have not studied HHS' enforcement actions; however, I think it has been widely reported that there have been few enforcement actions on their part.

The way HIPAA is set up right now is that if an individual has a complaint they can go to HHS, the Office of Civil Rights, and complain about privacy violations. I think that this, again, is another issue for us moving forward. Under HIPAA, for example, there is no individual right of action. If someone isn't satisfied with what happens at HHS, they cannot go to the courts for resolution. I think this is an issue that, you know, we will need to look at over time, but we haven't studied it in depth.

Mr. CLAY. One IT-specific recommendation offered by the National Council of Vital Health Statistics was for HHS to support research and development of contextual access criteria that is appropriate for the dissemination and sharing of electronic health information. Do you know whether HHS is addressing this issue and, if not, why not? And does GAO concur with the findings and rec-

ommendations of the National Committee on Vital Health Statistics?

Ms. KOONTZ. First of all, in terms of the contextual information, I think that is quite an exciting idea, because if you look at paper records right now, if you have to disclose a paper record I think that the default is to perhaps disclose the whole piece of paper. The idea of this contextual access would be that when you disclosed information you would use technology in such a way that you could disclose only the information that was actually needed, so it would be a way to really leverage technology to increase privacy for patients and consumers. So the National Committee on Vital and Health Statistics did recommend that HHS look at this more fully in the process, and we support that.

I think one of the things that, as they move forward on a comprehensive strategy for addressing privacy, they need to take into consideration the results of all these different contracts and initiatives that they have going on, which seem to have a lot of merit. They need to take into consideration the recommendations of NVCHS, and they need to take into consideration some of the challenges that I think we raised in our report.

Mr. CLAY. Thank you for that response.

When multiple States with conflicting laws have personal health information concerning the same patient, which State's privacy standard will apply, and under what circumstances? How can entities in one State appropriately manage patient data within their electronic patient records if they are unaware of applicable restrictions in another State?

Ms. KOONTZ. Well, the issue about HIPAA is that HIPAA is meant to be a floor in terms of privacy protection, so that means it does not preempt a State law that provides greater privacy protections than the Federal law. But you are right: what it leads to is very much a patchwork of different kinds of laws in varying States, and when you go to electronic health records and you go to a national health information network, again, the information is to move. It can move much more freely than it does now in a paper environment.

One of the challenges, when we were doing our study, that many organizations talked to us about is operationalizing these various requirements and being able to navigate in an environment where information is created in one State, it is sent to another, it is sent yet to another, and how to really navigate in that kind of environment has caused a complexity which may indicate some need maybe for greater guidance in terms of how to navigate this. And some people have suggested, of course, that there be some kind of national standard for privacy that is consistent across the States. We haven't studied that further, but that has been an issue that has often been raised.

Mr. CLAY. Good. Thank you very much.

Mr. Turner.

Mr. TURNER. Thank you, Mr. Chairman.

We want to note that Government Health IT reported on June 15, 2007, that Dr. Kolodner, National Coordinator of Health Information and Technology, has revealed that his office will propose a draft framework for privacy policy later this year. Kolodner said it

will reference other privacy policy documents from organizations such as Connecting for Health, the National Committee on Vital and Health Statistics, and the Organization for Economic Cooperation and Development. I look forward to seeing that so we can all have an opportunity to review it and determine its effectiveness.

I am going to ask if you could talk for a moment—and you may not be able to—but the VA's experience during Katrina, we have all heard news reports about how the VA was able to transfer large numbers of patients' records far more quickly than private hospitals. Are you familiar with the VA's experience and their system? Could you comment on that?

Ms. MELVIN. I am not familiar with that particular experience, but what I can tell you is that VA does have a comprehensive longitudinal electronic health record for its patients, which would explain its ability to make information available for those people who were affected by Hurricane Katrina. Its system is set up so that it contains a complete record of each patient that is captured within its system, so that would explain its ability to perhaps have records available more readily certainly than other entities that do not have such a capability at this point.

Mr. TURNER. Are you familiar with either their experience of cost savings or efficiencies in increasing medical care and/or privacy issues and policies?

Ms. MELVIN. I don't have specific information on their cost savings. I can tell you, though, that they have a very impressive system in place that has allowed them to achieve many improvements in quality of care through the clinician's ability to have ready access to information, through their ability to actually use that information in the health care of patients at this point.

Mr. TURNER. Thank you very much.

Ms. MELVIN. You are very welcome.

Mr. TURNER. Thank you, Mr. Chairman.

Mr. CLAY. Thank you, Mr. Turner.

Mr. Hodes, any more?

Mr. HODES. Just one more briefly.

Mr. CLAY. Please proceed.

Mr. Hodes. Thank you, Mr. Chairman.

I would like to followup just a little bit on the question about varying State standards, because I note at page, I think it looks like 15 of your report, where you talk about the challenges to exchanging electronic health information and the area of understanding and resolving legal and policy issues, and the first bullet point you talk about is resolving uncertainties regarding the extent of Federal privacy protection, and it leads me to the question of how quickly we can go to a national information system with so many differing standards out there among the States.

Could you tell us what do you think the benefits would be to establishing a Federal standard in these areas, even if it meant hypothetically preempting the States?

Ms. KOONTZ. Well, it is obviously a policy judgment that you are probably in a much better position to make than I, but——

Mr. HODES. That is why I asked the question.

Ms. KOONTZ. Fair enough. But, I mean, the obvious advantage here is that we would be trading off some, getting rid of some com-

plexity in order to, you know, if we got some standardization. Obviously, from talking to a fairly large number of entities out there who are involved in information exchange and involved in providing health care, it is tremendously confusing, even to the point of trying to decide what rules apply, what category do they fit in, and then also how to operationalize all the different kinds of requirements, as well. So, I mean, I can see on balance it is on the one hand and on the other hand, but there are definitely benefits to standardization, as well, although there may be States where you might end up lowering privacy protection, and I think that is an issue for that locality.

Mr. HODES. OK. Thank you very much.

Thank you, Mr. Chairman. I yield back.

Mr. CLAY. Thank you, Mr. Hodes.

The AHIC, which is a public/private working group chaired by the Secretary, assembled a working group on how to address privacy and confidentiality issues last August. What findings, if any, have been presented to the Secretary? Is AHIC's work consistent with GAO's findings and recommendations? Are you familiar with AHIC, the American Health Information Community?

Ms. MELVIN. Yes, we are familiar with that. As far as their findings and recommendations, at this point we are not certain as to exactly what they are doing. We do know that HHS is in the process of assessing the information that they have from them, and we have not compared that to GAO's recommendations, as I recall.

Mr. CLAY. OK.

Ms. MELVIN. We have not compared them to GAO's recommendations.

Mr. CLAY. All right. I thank you for that.

Let me thank both of you for your answers today and for being witnesses at this hearing. I think it is such an important issue, and we certainly appreciate GAO weighing in. Thank you both. This panel is dismissed.

I would now like to invite our second panel of witnesses to come forward, please.

Testifying today on our second panel will be Mary R. Grealy, president of the Healthcare Leadership Council. Welcome to you.

Bryan Pickard, president of the American Health Information Management Association. Thank you for being here.

Peter P. Swire, the C. William O'Neill professor of law at the Ohio State University's Moritz College of Law and senior fellow at the Center for American Progress.

Welcome to all of you.

It is the policy of the committee to swear in all witnesses before they testify. At this time I would like to ask you all to stand and raise your right hands.

[Witnesses sworn.]

Mr. CLAY. Let the record show that all of the witnesses answered in the affirmative.

Each of you will have 5 minutes to make an opening statement. Your complete written testimony will be included in the hearing record. The yellow light in front of you will indicate you have 1 minute remaining. The red light will indicate that your time has expired.

Ms. Grealy, we will begin with you. You may proceed.

STATEMENTS OF MARY R. GREALY, PRESIDENT, HEALTHCARE LEADERSHIP COUNCIL; BYRON PICKARD, PRESIDENT, AMERICAN HEALTH INFORMATION MANAGEMENT ASSOCIATION; AND PETER SWIRE, SENIOR FELLOW, CENTER FOR AMERICAN PROGRESS

STATEMENT OF MARY R. GREALY

Ms. GREALY. Thank you, Mr. Chairman and members of the subcommittee. On behalf of the members of the Healthcare Leadership Council, I want to thank you for the opportunity to testify on this extremely important subject.

Certainly all Americans want to be assured, as we move toward a day when virtually all clinical health information will be exchanged electronically, that their confidentiality will be protected and information will be used to provide health care of the highest quality.

The Healthcare Leadership Council is comprised of chief executives of many of the Nation's leading health care companies and organizations representing all sectors of American health care. Our members are some of the early adopters of health information technology.

Mr. Chairman, with my time limitations there are two key points that I would like to make today. First, allow me to comment on the current HIPAA privacy rule, a rule that was developed through careful, detailed deliberations over a 5-year period, and its effectiveness in the context of electronic health information exchange.

We are concerned that the transition to more widespread use of electronic medical records will prompt a reactive call in some quarters for additional burdensome privacy regulations. It is important to note that the HIPAA privacy rule, which is already quite restrictive, was spurred by the growth of electronic transactions and already contains ample provisions governing the confidentiality of information, electronic or otherwise. It is even more important to recognize that more-restrictive rules, such as requiring providers and payers to obtain prior consent for treatment, payment, and health care operations, would delay and disrupt health care, particularly for the most vulnerable patients.

The fact is, Mr. Chairman, the HIPAA privacy rule has a successful track record, and that success is being achieved in an environment in which multi-State electronic data exchange is already occurring.

Health care providers and plans have spent significant resources to comply with the HIPAA rule. Before considering any changes, we should be certain that they are absolutely essential and would warrant diverting finite resources from patient care to additional administrative compliance.

The other point I wish to make this afternoon is that, while the HIPAA privacy rule is effective in protecting patient confidentiality, the development of a multi-State network requires the creation of a uniform Federal privacy standard. While HIPAA establishes such a standard, it permits State variations that are found in thousands of statutes, regulations, common law principles, and

advisories. This patchwork quilt creates confusion among those who hold identifiable health information and those who seek to establish these data exchanges.

We believe strongly in a national standard that provides strong privacy protections for every American and facilitates nationwide and system-wide electronic data exchange for the betterment of patient care.

Mr. Chairman, Section 6 of your bill, H.R. 4832, laid out a process to help achieve that national standard, and we hope that it will find its way and be part of any future HIT legislation.

One thing that helps us put a face on health care policy and to put it in perspective is that these issues unavoidably become personal for all of us. My family currently has a compelling example in the person of my 88 year old father, who lives in Fort Lauderdale, FL. Just a few months ago, after a brief hospital stay for acute kidney failure, he began a regimen of dialysis three times a week. At the same time, he was receiving radiation treatment for prostate cancer.

I can tell you firsthand that the staffs in the hospital, the radiation center, the dialysis center, and the various physician offices are fully complying with the HIPAA privacy rules, oftentimes making it difficult for me and my five brothers and sisters to help coordinate his care. Be assured that health professionals take the rules very seriously.

More importantly, however, I am also experiencing firsthand the absolutely critical need for a unified electronic health record so that my Dad's oncologist, nephrologist, internist, cardiologist, nutritionist, radiation center, and dialysis center would all know in real time what each is prescribing and, more importantly, how he is doing. For example, sharing the results of lab tests, sharing the prescriptions that they are ordering.

An electronic health record would have avoided my Dad's recent experience of receiving Procrit from his oncologist while he was receiving a similar medication, Epigen, at the dialysis center. Unfortunately, it fell to us to alert and notify those two health providers, because they were not sharing this information.

You can see the importance of having this electronic health record. America's patients, not just my Dad, need electronic health record, and I applaud the efforts that you, Mr. Chairman, and others have put toward achieving that goal.

We look forward to working with you, finding the appropriate balance between privacy and the need for sharing this important information as we move forward in this important area.

Thank you.

[The prepared statement of Ms. Grealy follows:]

Testimony of

Mary R. Grealy
President
Healthcare Leadership Council

Protecting Patient Privacy in Healthcare Information Systems

Before the

House Committee on Oversight and Government Reform

Subcommittee on Information Policy, Census, and National Archives

June 19, 2007

I want to thank you on behalf of the members of the Healthcare Leadership Council (HLC) for the opportunity to testify before the House Committee on Oversight and Government Reform Subcommittee on Information Policy, Census, and National Archives on the Health Insurance Portability and Accountability Act of 1996's (HIPAA) privacy rule and how it will protect patient privacy in an environment of electronic clinical health information exchange.

HLC is a not-for-profit membership organization comprised of chief executives of the nation's leading health care companies and organizations, with membership that includes hospitals, health plans, pharmaceutical companies, medical device manufacturers, biotech firms, health product distributors, pharmacies and academic medical centers. Fostering innovation and constantly improving the affordability and quality of American health care are all goals uniting HLC.

The Healthcare Leadership Council supports the Administration's goal that most Americans have electronic health records by 2014. And we appreciate the bi-partisan commitment by Congress to encourage widespread adoption of health information technology.

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

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

health care; contribute to greater patient safety and better patient care; and achieve clinical and business process improvements.

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

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

Given the time that has elapsed since development of the HIPAA privacy rule, I think it would be useful to revisit the deliberations about confidentiality during development of the rule. Those intensive, comprehensive deliberations over a five-year period carefully weighed the competing interests in our extraordinarily complicated health care system. They included both a Democrat and Republican Administration and thus experts from both political parties. The result of these deliberations we believe to be an effective privacy rule.

For more than ten years, HLC has chaired the "Confidentiality Coalition,"[1] a broad-based group of organizations that support nationally uniform privacy standards. During Congressional enactment of the (HIPAA) statute and regulatory development of the HIPAA Privacy Rule, the Confidentiality Coalition played a leadership role, working with members of Congress and the administration to advocate for a workable privacy

[1] The Confidentiality Coalition includes over 100 physician specialty and subspecialty groups, nurses, pharmacists, employers, hospitals, nursing homes, biotechnology researchers, health plans, pharmaceutical benefit management and pharmaceutical companies.

rule. Today, the Coalition continues to help educate members of Congress about the protections afforded in the Privacy Rule to avoid conflicting or duplicate legislation.

During deliberations on the Privacy Rule, we sought a rule that would strike the appropriate balance between protecting the sanctity of a patient's medical information privacy while, at the same time, ensuring that necessary information is available for providing quality health care and conducting vital medical research. We advocated for a rule with effective confidentiality safeguards that would not burden providers and patients with unnecessary paperwork or delays in treatment. We believe that the Privacy Rule to a great extent achieved this balance and has increased consumers' confidence in the privacy of their medical records. We thus are especially interested in how these successes will affect efforts to achieve interoperable health information exchange, and how flexibly the rule works for a fully, or even partially, electronic health care system.

Covered entities take compliance with the Privacy Rule very seriously. Health care providers, payers and other covered entities as well as their business associates have implemented comprehensive training and compliance plans to adhere to the Privacy Rule. Under the Privacy Rule, disclosing identifiable health information for purposes other than carefully defined, appropriate health-care activities is prohibited unless the patient grants specific, prior written authorization. The statute carries strong civil and criminal penalties for non-compliance.

Some have suggested that enforcement and penalties for violations of the HIPAA rules are not adequate. However, in evaluating HIPAA compliance and enforcement, it is important to note that the HIPAA Administrative Simplification Enforcement Final Rule was only recently promulgated on February 16, 2006. The Final Rule adopts the complete rules for enforcing all of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act including the privacy, security, transactions and code sets, and identifier rules. In addition, the Final Rule establishes uniform investigation and hearing procedures to make the enforcement process operate

more efficiently. Thus, HHS has only recently had the necessary tools to enforce the rule.

I might also note that the Office of Civil Rights (OCR), charged with overseeing the privacy rule, has partnered with providers and consumers to educate them on how to comply with the rule. OCR has found that many alleged violations were really misunderstandings of the complex HIPPA rule – rather than intentional breaches of the rule's requirements.

In addition, since April of 2005, covered entities must also be in compliance with the HIPAA Security Rule. The Security Rule applies to electronic protected health information that a covered entity creates, receives, maintains, or transmits. The rule requires covered entities to protect against threats or hazards to the security or integrity of information, as well as uses and disclosures not allowed by the privacy rule.

Ongoing dialogue about health information technology and standards for the electronic transaction of health care has raised questions about the privacy and security of electronic health information in an electronic context. I think it is of the utmost importance to note that it was concern about the impact on patient privacy of the health system widely adopting *electronic* transactions that spurred the HIPAA privacy rule. Thus, during the rulemaking process for the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security rules, many of these same questions were discussed, and the result is that the HIPAA Privacy and Security rules include ample provisions governing the confidentiality of patient medical information, electronic or otherwise.

We are concerned that some policymakers may not be aware of the purpose and scope of the HIPAA privacy and security rules and will advocate for additional, burdensome privacy regulations for electronic health records. The current HIPAA regulations are very restrictive and companies like our members have taken a very conservative compliance approach in their business practices. I think many consumers will attest to

this fact if they have attempted to get health care claims or medical information for themselves or another person, such as a parent, without a prior approved authorization. Some have expressed concerns about "hyper-compliance" with the privacy rule.

We understand that many believe that the HIPAA privacy rule must be revised in light of electronic transfer of data and web-based access to personal health records, so that patients may trust that the system will keep their data private. We share the belief that patients' confidence in health information technology systems is of the utmost importance in order for them to be successful. We believe that it is vitally important that patients understand the protections contained in the HIPAA rule, so they can be confident that their records are and will be protected.

We must all do a better job of educating the public as to how electronic health records will improve the quality, safety and efficiency of their health care and that of future generations. More importantly they must know the steps taken to keep their information secure and that it cannot be disclosed to their neighbor, their employer, or the newspaper without their express written permission.

I. National Uniform Standard for Privacy

One area of concern regarding the privacy rule is the rule's lack of a national uniform standard for privacy. Though we strongly believe that the HIPAA privacy rule provides a sound basis for protecting health information, progress toward electronic data exchange is significantly impeded by the lack of a uniform federal privacy standard.

As an underpinning for our discussion today, we've attached a map developed by the Indiana Network for Patient Care (Fig.1). Each dot represents a patient seen at an Indianapolis hospital during a six-month period. While the dots are stacked very deep around Indianapolis as you would expect, patients served by the Indiana hospitals during this period were also residents of 48 of the 50 states. Today's health care providers, meeting the needs of a mobile society, serve patients from multiple and far-

flung jurisdictions. Looking at this map it is easy to see why local and regional agreements will not be adequate to address the myriad regulations with which providers and others will need to comply to achieve interoperability and why national standards, for interoperability as well as privacy and data security, are necessary.

Although HIPAA establishes a federal privacy standard, it permits significant state variations that we believe will create serious impediments to interoperable exchange of health information, particularly across state lines. This is true not only with respect to the technical standards employed through information technology, but also with respect to the privacy standards that govern information disclosures.

In addition, since the Privacy Rule does not supersede state privacy laws, providers, clearinghouses and health plans are required to comply with the federal law as well as any state privacy restrictions that are contrary and more stringent. In the context of HIPAA implementation this has been extremely difficult and in the content of broad and widespread health information exchange it may be nearly impossible.

State health privacy protections vary widely and are found in thousands of statutes, regulations, common law principles, and advisories. Health information privacy protections can be found in a state's health code as well as its laws and regulations governing criminal procedure, social welfare, domestic relations, evidence, public health, revenue and taxation, human resources, consumer affairs, probate and many others. While Indiana uses HIPAA as its state privacy law, virtually no other state's requirement is identical to the federal rule. Within a given state, privacy laws may actually conflict, adding to confusion among those who hold identifiable health information and those who seek to set up data exchanges.

HHS will not provide a comprehensive preemption analysis of these state privacy protections. Moreover, single-state and private-sector efforts have been extremely costly, do not utilize consistent standards, and are difficult to manage against the constantly changing 50-state environment. HLC and the Confidentiality Coalition

attempted to address this problem directly by commissioning a multi-jurisdiction study of this issue and quickly assessed costs of more than $1 million with $100,000 for annual updates. Unfortunately many organizations, particularly smaller provider groups, do not have such resources and must navigate the sea of privacy regulations and laws on their own.

Several projects at HHS are currently studying state privacy laws and determine their potential impact on health information exchange. In October of 2005, the Agency for Health Research and Quality (AHRQ) awarded a contract to RTI International to assess the variations that exist at the organization level with respect to privacy and security practices and policies.

The federally funded RTI study is looking at 33 states and focusing on working with state organizations to determine what laws exist in each state and what organizations are doing to streamline state statutes and regulations to make them consistent within each state, so that data may be exchanged more easily within a given state. But looking at the Indiana chart referenced above, it is unfortunate that the RTI study did not do a thorough analysis of how state laws are impeding movement of information across state lines.

From the discussions of RTI study participants at its March conference on Privacy & Security Solutions – which convened the state officials and project managers involved in the RTI study – it appears that even within each state many organizations are unable to discern the appropriate statutes and regulations. In summary, state stakeholders are identifying a general misunderstanding regarding the many potential intersections of present state laws and HIPAA, finding that state laws do not currently address or apply sensibly to the proposed electronic exchange of health information. Instead, stakeholders suggest that their legal departments seem simply to establish a privacy policy with which they are comfortable, refusing to exchange data with any but trusted partners. While this is completely understandable in the context of the wide range of

state laws and regulations, it bodes poorly for electronic data exchange, especially across state lines.

How can each physician's office, hospital, and clinical lab develop relationships as a trusted partner with the thousands or more other entities who could participate in clinical data exchange? While organizations such as the Markle Foundation are working with local and regional health information exchanges to craft an acceptable, standardized trusted-partner contracts, this local resistance to exchanging information with any but trusted partners is seriously impeding health information exchange. A quicker way to alleviate the concern would be to establish one federal privacy standard that assuaged all entities' fears about who could be trusted.

Interestingly, the exception may be Indiana, where, because HIPAA essentially serves as the state's health privacy law, the state is proceeding with a state-wide health information exchange. In many ways, Indiana serves as a state model for how more easily an electronic health information exchange could be established with a single privacy standard.

The RTI project is not the only HHS sponsored entity studying state variations in privacy. In October of 2006, HHS' Office of the National Coordinator for Heath Information Technology (ONC) announced that it had entered into a one year, $1.99 million dollar contract with the National Governors Association's (NGA) Center for Best Practices to establish the State Alliance for e-Health. The State Alliance will serve as a forum in which state-level consensus-based solutions can be developed to address key challenges to interoperable health information technology. Privacy and security issues will be addressed by the alliance along with other state policy issues impeding health information exchange.

HLC is not alone in calling for nationally uniform privacy standards. The 11-member Commission on Systemic Interoperability, authorized by the Medicare Prescription Drug, Modernization, and Improvement Act to develop recommendations on HIT

implementation and adoption, recommended that Congress authorize the Secretary of HHS to develop a uniform federal health information privacy standard for the nation, based on HIPAA and preempting state privacy laws, in order to enable data exchange interoperability throughout the country.

While we believe strongly in the need for a national privacy standard, HLC believes just as strongly that any regional or national system designed to facilitate the sharing of electronic health information must protect the confidentiality of patient information. It is not our intent in calling for one national privacy standard to weaken privacy protections for individuals, but rather to facilitate nation- and system-wide electronic interchange of data.

II. Patient Consent and Control

You have asked us to address the effectiveness of current laws and regulations governing use and disclosure of information in the context of electronic health information exchange. At the center of the dialogue about electronic health records and information is the question of patient consent and control. After lengthy debate, the final HIPAA Privacy Rule as modified allows covered entities to use patients' medical information without authorization for medical treatment, claims payment or health care operations or as otherwise permitted or required[2]. For other uses, providers must obtain a written authorization from each patient.

Requiring providers and payers to obtain prior consent to use individually identifiable health information for treatment, payment and health care operations was rejected because of concerns that a prior authorization requirement would seriously delay and disrupt the care of patients, particularly the most vulnerable patients. For example,

[2] Under the Privacy Rule a covered entity is permitted to use and disclose protected health information without authorization for the following purposes or situations: 1) to the individual; 2) for treatment, payment and health care operations; 3) for uses and disclosures with an opportunity to agree or object; 4) for uses and disclosures that occur incident to an otherwise permitted use or disclosure; 5) for public interest and benefit activities; and 6) of a limited data set for purposes of research, public health or health care operations.

elderly patients would not be able to send a family designee to a pharmacy to pick up a prescription without first going to the pharmacy to sign consent forms; pharmacies would not be able to fill prescriptions phoned in by physicians until the patient arrived to give consent; and emergency medical personnel would be forced to get consent forms signed before treating patients – even when contrary to best medical practice. These concerns were not simply theoretical; Maine enacted a law requiring prior consent to use patient-identifiable information for health care purposes. The law was suspended just 12 days after taking effect because of the chaos that ensued in hospitals and pharmacies.

The much-touted benefits of health IT, most importantly improvement of quality of care through better patient incomes, will not be realized if information exchange is constrained by various authorization or consent requirements. Far worse, adding such requirements in the context of health information exchange will slow and impede providers' current ability to deliver health care services. Thus, in general, we believe that changing the rule's provisions regarding consent and control would be unnecessary and harmful.

In recent years, the advent of personal health records (PHRs) has triggered another set of discussions about patient control of their health information. We agree that with respect to PHRs, individuals will want to control distribution. We are seriously concerned about the prospects of allowing consumers to control which health care providers may see their medical records and the portions of the records that may be shared, even after the patient has entered the health care system for treatment. We caution against allowing or expecting a fully patient-controlled PHR to become a *de facto* electronic health record for use in clinical settings, as physicians will never trust that they have accurate and complete information if they know that patients can withhold pieces of the record.

We would suggest that while PHRs may be controlled by individuals, once their information reaches an EHR, it should be used and disclosed as under HIPAA, allowing

for information to move within the health care system, including via electronic data exchange, as it may under HIPAA, which will facilitate optimal patient care and data available to improve health care quality.

If patients may direct where information may flow within the health care system, it will upset HIPAA's careful calibration, designed to facilitate providers having all the necessary facts for proper diagnosis and treatment. Enabling patients to direct what information may be shared electronically is the same as saying patients may direct what information is withheld from their physicians, researchers and accreditors. Critical data could be omitted from aggregated data made available to researchers hoping to improve health care quality and patient outcomes. In addition, providers are very concerned about the liability that might result from their reliance on incomplete information.

We often hear the argument that physicians already are relying on incomplete information and that at least a partial record would be an improvement. We would respond that given the resources that will be required to implement health IT, it would be irresponsible to build into a new, more expensive medical records system the same drawbacks that are inherent in our current, largely paper-based system. If we want to retain the inefficiency and lack of data of the current system, the nation does not need to spend billions of dollars on health information technology.

We agree that use of a national, regional, or even local health care information exchange will require patient and consumer confidence. It will be crucial to educate consumers and patients about the privacy protections and penalties enacted under HIPAA and the Security Rule. However, providers too must have confidence in the integrity of the data provided through health information exchange in order to assure utilization of such a system. In evaluating proposals to require consent or varying degrees of patient control, we urge the Subcommittee to carefully consider the ramifications for health care delivery and public health that such steps would impose.

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

III. HIPAA Expansion in Health Information Exchange

As participants throughout the process of developing first HIPAA and then the privacy rule, we believe that policymakers worked diligently to foresee how information would move in the coming years. Indeed, the rule works very well for health information exchange within HIPAA covered entities and activities.

In addition, other entities beyond HIPAA covered entities comply with the privacy rule's requirements. "Business Associates" of covered entities, those that perform certain functions or activities on behalf of a covered entity, or provide services to a covered entity that involve the use or disclosure of individually identifiable health information, are contractually bound to the rule's standards and thus are contractually prohibited from making any use or disclosure of protected health information that would violate the Privacy Rule.

What the rule did not contemplate was the broad movement to web-based technology, instead of electronic medical records housed within providers' offices or at hospitals. In an internet-based world, many organizations may have access to protected health information, some without the patient's knowledge. Those that are not already complying with HIPAA, either as a covered entity or business associate, should be included as HIPAA-covered entities. For example, health information exchanges could be regulated as HIPAA-covered entities if they cannot be determined to qualify as health care clearinghouses.

Regulation of personal health records (PHRs) is somewhat less clear. Under current scenarios, individuals give PHR companies permission to hold their data, which the company maintains for them in a record, and which the company will send to clinicians

and health care providers upon the authorization of the patient. To date, the companies providing PHRs include health plans, stand-alone organizations, and divisions of larger, diversified companies who may not be health care companies. To the extent that these records are held by health plans, they appear to be captured under HIPAA. To the extent that they are not held by health plans, they are essentially unregulated, other than through the contractual agreements that the companies have with the individuals whose records they hold.

It is in the companies' best interests to keep identifiable information confidential, and to date, they all profess to adhere to extremely strict privacy standards. Assuming that the value of the record is in its storage and transmission, we can expect companies to adhere to their strict privacy protections. Should the value of the records for other purposes exceed their value for maintenance and distribution, then the records are somewhat less likely to be kept confidential.

The HLC would support reasonable efforts to ensure that personal health records held by organizations that are not HIPAA-covered entities meet HIPAA privacy and security rule requirements. The challenge, however, is how to structure such a requirement.

One possibility would be to deem health information exchanges as health care clearinghouses for the sake of simplicity.

The ramifications of extending HIPAA coverage to other entities must be carefully considered, but we strongly believe that to the extent that additional entities are brought into federal privacy protections, it is critically important not to upset the carefully calibrated balance HIPAA has struck with respect to access to information and confidentiality.

HLC has some additional concerns about how well the HIPAA privacy rule functions, but given the questions you have asked us to address in this meeting, we have reserved them in an addendum to the testimony.

Conclusion

In conclusion, I want to thank you again for the opportunity to testify before the Subcommittee. HLC strongly supports the broader implementation of HIT – HIT offers unparalleled potential for improvement in health care quality. However, patients' confidence in the confidentiality and security of the HIT infrastructure that is built is essential in order for the resources spent on HIT acquisition and development to be meaningful.

We would urge the Subcommittee's careful consideration of the ramifications of changes to the federal regulations governing patient confidentiality. Such changes, if any, should be measured and deliberate in order to continue the successful track record set by the HIPAA privacy rule.

Health care providers, plans and clearinghouses have spent significant resources to comply with the HIPAA privacy rule. Before recommending changes to the rule, we should be absolutely certain that such changes are indeed necessary in order to justify the diversion of scarce resources from patient care to administrative compliance.

Multi-state electronic exchange of data is already occurring, as health plans, pharmacy benefit managers, pharmacists use their interconnected electronic systems to pay claims, fill and pay for prescriptions, operate disease management programs, and alert patients and clinicians to important information. While patients and clinicians are as yet unused to accessing medical files electronically, the HIPAA privacy and security protections for identifiable information have worked very well to keep patient-identifiable information confidential. There is no reason to believe that these same protections, which were drafted with the electronic transmission of health care treatment and patient information in mind, will not work equally well for expanded exchange of clinical information.

We look forward to continued work with the Subcommittee. Any questions about my testimony or these issues can be addressed to me at the Healthcare Leadership Council (telephone 202-452-8700, e-mail mgrealy@hlc.org).

Addendum: Other concerns about HIPAA's current requirements in the context of HIT

IV. Minimum Necessary

HLC believes that the Privacy Rule's minimum necessary standard – which already poses significant burdens for covered entities – may be unworkable in the context of disclosures made through health information exchange from health care providers. The Privacy Rule provides that covered entities must make "reasonable efforts" when using, disclosing or requesting protected health information, to limit the information to the "minimum necessary" amount needed to accomplish the intended purpose of the use, disclosure or request. In addition, the regulation provides that covered entities may not use, disclose or request an entire medical record unless the entire record is "specifically justified" as the amount of information reasonably necessary. Disclosures to, or requests by, a provider for treatment purposes are exempt from the standard as are uses or disclosures made pursuant to a written patient authorization. A covered entity may rely on a requested disclosure of protected health information from another covered entity as being the minimum necessary amount.

This standard puts covered entities receiving requests to disclose information in the position of determining whether the requested information is the "minimum necessary" amount, when only the entity making a request for information has an informed basis for determining whether the information is the minimum necessary for its purposes. The legal uncertainty and risk created by this standard already has led to some "defensive" information practices that restrict the appropriate flow of information within the health care system. For example, some providers, citing the need to comply with the HIPAA Privacy Rule, have limited access by health plans to protected health information needed to perform quality assessment and improvement programs, utilization review, case management, disease management, and other functions related to maintaining the affordability of health coverage and improve outcomes.

Especially in an era of increasing interest in comparing the effectiveness of treatments, it is critically important that information be available to those who may legally access it for legitimate reasons, such as determining the relative effectiveness of one treatment versus another, and that patient control of information or citations of the minimum necessary requirements not be used to subvert attempts to determine optimal and efficient treatments for patients.

For participants in a national or regional health information network, making minimum necessary determinations – or even determining if a requesting party or provider is a HIPAA covered entity – is likely to be extremely challenging. The uncertainty and resultant liability exposure associated with the minimum necessary standard is likely to serve as a barrier to participation in health information exchange. Interoperability and information exchange across healthcare settings cannot be fully met if a physician is required to adhere to a nebulous minimum necessary standard. The application of the minimum necessary standard to this effort may in fact increase medical error rates by limiting the flow of medical information in the health care system in a manner that is inconsistent with the provision of quality medical care. Consideration should be given to eliminating the standard, or creating a safe harbor for when personal health information is exchanged through a national health information network or regional health information exchange.

V. Research

We are also concerned that current-law restrictions in the area of research will prevent health information exchange from achieving its ultimate objective as a tool to improve quality of care.

Research uses and disclosures are an essential part of the national HIT infrastructure envisioned in many scenarios, especially as it pertains to improvement of patient care. The data collected in this effort will be crucial to achieving key objectives of this initiative,

particularly the goal of improving population health by accelerating the movement of the fruits of research into delivery systems in a meaningful way.

The HIPAA Privacy Rule also recognizes the importance of research to improving the quality of health care and took steps to ensure that researchers would have continuing access to health information. Under the Privacy Rule, numerous entities, including non-covered entities, receive and analyze de-identified data or limited data sets to assist health care providers, health plans, government, the health care management communities and manufacturers conduct market, utilization and outcomes research, implement best practices, and apply and benefit from economic analyses. Data researchers have helped implement prescription drug recall programs, performance of pharmaceutical market studies, and assessment of drug utilization patterns. In these areas and many others the HIPAA framework took care to protect patient privacy while permitting data use for research where appropriate.

We are concerned, however, that in some instances the HIPAA Privacy Rule failed to achieve the proper balance and is inappropriately restricting access to health information for researchers. In particular, requiring expiration dates or events on all research authorizations and prohibiting individuals from granting authorization to use their health data in unspecified future studies is limiting the on-going use of research data in ways that are detrimental to the health care system. Under the Common Rule that has governed human subject research for decades, it is generally permissible to obtain informed consent from a participant to use data for future research on data or biologic materials stored in databases or tissue banks. The Privacy Rule does not permit authorization for virtually any unspecified future uses. The Secretary's Advisory Committee on Human Research Protections (SACHRP) has recommended that the HIPAA Privacy Rule permit future uses that are allowed under the Common Rule. We agree that the Privacy Rule needs to be modified in this area to be consistent and note that these restrictions, if not addressed, will have a significant impact on the ability of stakeholders to achieve critical goals of HIT.

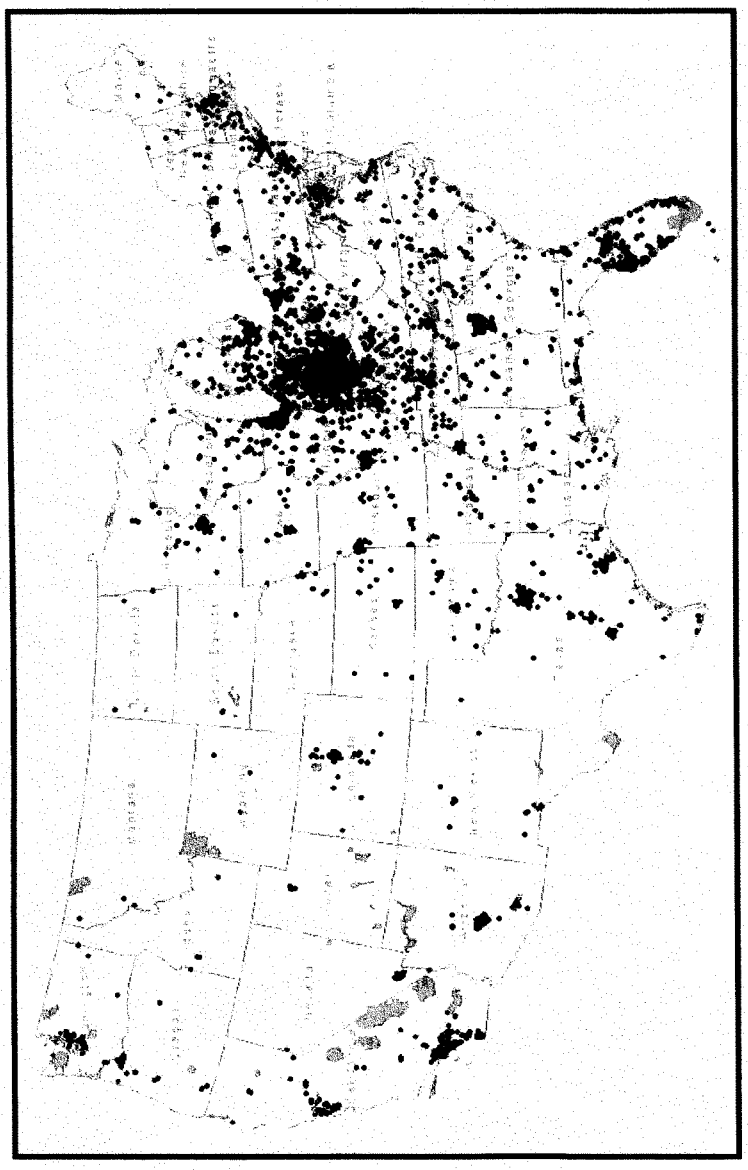


Fig. 1: Map prepared by Indiana Network for Patient Care, 2004. Dots represent home addresses of patients treated at an Indianapolis, IN hospital over a six-month period.

Mr. CLAY. Thank you so much, Ms. Grealy, for that testimony. Mr. Pickard, you may proceed.

STATEMENT OF BYRON PICKARD

Mr. PICKARD. Chairman Clay and members of the subcommittee, thank you for this opportunity to testify. I will be testifying on behalf of AHIMA, but will also draw upon my professional experiences to describe the public/private efforts currently underway exploring the privacy of electronically transmitted health information.

My written testimony addresses some areas of specific interest to our profession; namely, expansion of privacy protections for personal health records, differences between HIPAA at business associates and non-covered third-party contractors, and protecting student health information, and conflicts between HIPAA and FERPA. AHIMA also has a foundation of research and education, which has received several grants and contracts from the Office of the National Coordinator and others. I have attached a list of those commitments.

Mr. Chairman, the HIM professionals' responsibilities are interwoven with privacy and security issues. The expansion of confidentiality management and protection is impacted not only by HIPAA but also by the health care industry's continued transformation from a paper intensive industry to one of electronic records and transmissions.

I wish I could tell you that the health care industry has been transformed into a fully electronic system, but, in fact, I cannot. We are in the midst of what would be a long transition.

In working through these transitional issues, AHIMA has partnered with the American Medical Informatics Association and we have produced two joint statements relative to today's discussion, one on health information confidentiality, and the other on the value of personal health records. With so much history and experience in the protection of health information, it is important to note AHIMA's position. Our written testimony contains our full list of health information confidentiality principles.

As our health care system becomes more interconnected, our networked health information will flow across a range of entities and boundaries. It will be critical to follow these principles. Privacy protections must follow personal health information [PHI], no matter where it resides, and uniform and universal protections for PHI should apply across all jurisdictions in order to facilitate consistent understanding and compliance.

Considerable time has been spent exploring and developing electronic health information exchange and how to protect health information by the Agency for Health Care Research and Quality, a American health information community, the Office of the National Coordinator, and others. These initiatives and their impact on privacy and security are detailed in our written testimony.

AHIMA members, and especially those who fill the role of privacy office, are noting that the issue of confidentiality is moving beyond just health care. With the banking and finance industries handling health information more frequently, it has become apparent that we must soon address the comprehensive protection of an individual's information, White House whether it is financial or

health related. This is an issue that Congress will need to investigate as we see more change in the bordering of industry boundaries.

We also see a need for consumer education to address confidentiality and security, as well as the value of health information technology usage. It is only with consumer trust that a national infrastructure can be built and laws adopted or modified to facilitate information exchange.

AHIMA has long called for consumer-based personal health records, in addition to the standard provider-based electronic health records. While we have never endorsed a PHR product, we have called for consumers to use a PHR, whether in paper or electronic form, to track their own health status. To support this goal, AHIMA embarked upon a PHR consumer education campaign that combines the use of a consumer Web site with public presentations by AHIMA members in each and every State.

AHIMA is leading an effort to ensure interoperability of the PHR, with the new health level seven standard electronic health record, and we expect to see a new PHR electronic standard from HL–7 in the near future.

AHIMA's believe that protections should follow personal health information, no matter where it might be stored or transferred, clearly extends to PHRs. PHRs can be stored or offered by a variety of different vendors or operators. Some of these vendors are HIPAA-covered entities, and others are not.

Protections against the discrimination and misuse of PHR information must be established along with a requirement that any access or use of PHR information be governed by a separate authorization unless otherwise required by law. Except for PHRs offered by health care providers, we believe that individuals should be given the right to opt out of a PHR being built for them or their family members.

The answers are not simple. As the AHIC and the NCVHS and others discuss and provide recommendations in the privacy and security area, Congress can also begin to look at some very important issues: that confidentiality of protections follow the information no matter where it resides or is transferred; that comprehensive nondiscrimination laws have harsh penalties for the intentional misuse of health information; that we prosecute those who break these laws; that we penalize those entities that are non-compliant with confidentiality and security laws and regulations; that conflicts between HIPAA versus FERPA be eliminated in favor of consistent and strong confidentiality; and that proposed laws be reviewed to identify barriers that may arise that would impede the deployment of health information technology products, expansion of health information exchange, and critical uses of health information.

Mr. Chairman and members of the subcommittee, I hope that our testimony has given you an insight into the aspects of health care confidentiality and security that you are seeking, and that our recommendations will provide you with guidance as you address the many difficult questions facing our community. I stand ready to answer any further questions or concerns you might have.

Thank you.

[The prepared statement of Mr. Pickard follows:]

AHIMA
American Health Information Management Association

Testimony of Bryon Pickard, MBA, RHIA

President

American Health Information Management Association

to the

Committee on Oversight and Government Reform

Subcommittee on Information Policy, Census and National Archives

June 19, 2007

Introduction

Chairman Clay and members of the Subcommittee, thank you for inviting the American Health Information Management Association (AHIMA) to testify today on current privacy policies (HIPAA), and the challenge of integrating adequate privacy protections into a national health IT infrastructure. My name is Bryon Pickard, MBA, RHIA and I am the current President of AHIMA. AHIMA is the premier association of health information management (HIM) professionals whose more than 51,000 members are dedicated to the effective management and analysis of the health data and information needed to deliver quality healthcare. Founded in 1928 to improve the quality of medical records, AHIMA is committed to advancing the HIM profession in an increasingly electronic and global environment through leadership in advocacy, education, certification and lifelong learning.

In addition to my role as President of AHIMA, I am the director of operations for the Vanderbilt Medical Group Business Office at Vanderbilt University Medical Center in Nashville Tennessee. I have also participated in privacy, confidentiality and security design workgroups for the Vanderbilt Center for Better Health and e-Health initiatives focusing on regional and state-wide health information exchange projects in Tennessee. My experience also includes leading integration, merger and audit strategies for health information systems, registration and patient accounting applications, and I currently serve as a member of the practice management application IT advisory committee at Vanderbilt.

Today, I will be testifying on behalf of AHIMA but will draw upon my professional experiences at Vanderbilt and the previous environments in which I worked. My testimony will focus on the public private efforts underway to ensure the privacy of electronically transmitted health information and the effectiveness of our current laws and regulations governing the use and disclosure of such information. In addition, I will address some specific areas that are of specific interest to our profession and the reason for today's hearing:

- Expansion of privacy protections for personal health records
- Differences between HIPAA "business associates" and non-covered third-party contractors
- Protecting student health information: Health Insurance Portability and Accountability Act (HIPAA) vs. Family Educational Rights and Privacy Act (FERPA)

For almost 80-years, the HIM profession has strived to maintain the confidentiality of health records and be the patient's advocate within the healthcare system. It is with AHIMA's history and experience, along with my own, and those of the AHIMA members that I have met as an officer and director of AHIMA and the Tennessee Health Information Management Association (THIMA) that I come before you today prepared to respond to your concerns and questions on the confidentiality and security of health information.

For full disclosure, I must note that AHIMA is comprised of over 51,000 healthcare professionals affiliated with one of 52 state associations. In addition to a detailed academic curriculum, most AHIMA members are also certified in one or more areas of HIM, including a certification in privacy and security. AHIMA also has a foundation, the AHIMA Foundation for Research and Education (FORE), which is involved in a variety of research and academic scholarship endeavors. It is through

the reputation and experience of AHIMA members that FORE has received several grants and contracts from the Department of Health and Human Services' (HHS) Office of the National Coordinator for Health Information Technology (ONC). The grants and contracts are focused on state health information exchange analysis, the potential for fraud associated with electronic records, and subcontracts associated with the area of privacy and security. I have attached a list of those commitments to this testimony.

Mr. Chairman, the HIM professional's responsibilities are interwoven with privacy and security issues. With the advent of privacy and security rules associated with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), our profession undertook the role of addressing confidentiality and security as it relates to the electronic transmission of healthcare data—the use, access and disclosure of health information to persons other than the individual or the individual's representative. As you are aware, the adoption of the HIPAA privacy rule was not without considerable debate and the implementation took considerable time, effort, and resources.

The expansion of confidentiality management and protection was impacted not only by HIPAA, but also by the healthcare industry's continued transformation from a paper-intensive industry to one of electronic records and transmissions. I wish I could tell you that the healthcare industry has been transformed into a fully electronic system, but, in fact, I cannot. Rather we are in the midst of what will be a long transition that will see the introduction and implementation of a standard, electronic health record, personal health records, and health information exchange networks also called Regional Health Information Organizations (RHIO) or Regional Health Information Networks (RHINs).

In working through these transitional issues, AHIMA has often partnered with the American Medical Informatics Association (AMIA) to form what we believe is a responsible approach to the healthcare industry's transformation. I want to mention this relationship because AHIMA and AMIA have produced two joint statements relevant to today's discussion:

- The AHIMA-AMIA Joint Position Statement on Health Information Confidentiality
- The AHIMA-AMIA Joint Position Statement on the Value of Personal Health Records

With so much history and experience in the protection of health information and our involvement in the current transformation of our healthcare system, it is important to state AHIMA's position related to today's topic—current privacy policies (HIPAA) and the challenge of integrating adequate privacy protections into a national health IT infrastructure. First, any organization that accesses or stores personal health information should abide by the following principles:

- Inform individuals, through clear communications, about their rights and obligations and the laws and regulations governing protection and use of personal health information (PHI).
- Notify individuals in clear language about the organization's privacy practices and their rights in cases of security breaches
- Provide individuals with a convenient, affordable mechanism to inspect, copy, or amend their identified health information/records
- Protect the confidentiality of PHI to the fullest extent prescribed under HIPAA, regardless of whether the organization is a "covered entity" as defined in HIPAA, and ensure that the

organization and its employees all comply with HIPAA, state laws, and the policies and procedures put in place to protect PHI.
- Use PHI only for legitimate purposes as defined under HIPAA or applicable laws.
- Prohibit the use of PHI for discriminatory practices, including those related to insurance coverage or employment decisions.
- Timely notification of individuals if security breaches have compromised the confidentiality of their personal health information.
- Work with appropriate law enforcement to prosecute to the maximum extent allowable by law any individual or organization who intentionally misuses PHI.
- Continue to improve processes, procedures, education, and technology so that PHI practices improve over time.

As our healthcare system evolves and becomes more interconnected, health information will flow across a range of organizational, state and potentially international boundaries through a nationwide health information network structure. As we evolve into this structure, it will be critical to follow principles covering health information when it is transferred between entities and across boundaries:

- Health information privacy protections must follow PHI no matter where it resides.
- Uniform and universal protections for PHI should apply across all jurisdictions in order to facilitate consistent understanding and compliance by those covered by such laws and the individuals whose health information is covered by such laws.

Trends are Changing-Health Information Exchange

As members of the subcommittee are aware, a number of efforts are underway to address many of the issues we have discussed today. AHIMA, the healthcare industry, and those of us in Tennessee have spent considerable time and energy, as has the Congress, exploring and developing electronic health information exchange. Whether we call such an exchange a RHIO or an HIE, the concept of moving healthcare data electronically is a critically important topic that we have now discussed for a multitude of years. We have seen various groups agonize over how to protect health information, based on where it is stored, how it might be transmitted or accessed. They have also agonized over various protections for specific types of data as behavioral health, HIV, genetic information, and so forth. The importance of specific types of data is in the eye of the beholder. Our experience has indicated to us that all health information should be treated equally—specific policy protections for specific types of data can give away its type. Yes, you can build extra layers of security requirements in your systems to protect the data but specific policy requirements can cause problems.

The HHS Agency for Health Research and Quality (AHRQ) through its subcontractor RTI is finishing a research project - Health Information Security and Privacy Collaboration (HISPC) - that covered the privacy and security environment of some 34 states and territories. The final report from this project is due shortly and separate reports have been generated by the 34 states and territories, indicating where laws, regulations, and business practices related to privacy and security, potentially stand as barriers to the implementation of standard Electronic Health Records (EHR) and the exchange of electronic health information. Already, many of the groups that participated in this effort at the state level, have indicated that they have or will undertake additional efforts to address and resolve these barriers on a state level. At the same time, these same groups have indicated that such projects may take multiple

years. For instance, the group involved in Florida indicated that there are over 60 chapters of state law that need to be addressed to arrive at a uniform set of code to address health information privacy in that state. While we would like to see uniformity at the state, regional, and national level, we must recognize just what a large project this will be.

ONC, based on preliminary reports from the AHRQ effort, and the State HIE Best Practice Project (that AHIMA/FORE coordinated) has engaged the National Governors Association (NGA) to look at the potential to design uniform state laws or regulations that might bring us the uniformity and consistency needed for a national health information exchange system or network. The NGA effort began this last January. Included in the effort is a committee addressing the protection of health information. The NGA is aware that there are several more formal efforts that have already begun in the states by some individual governors. It is unclear if the governor's themselves are trying to keep their individual efforts open to national uniformity as they move forward.

Secretary Leavitt initiated the American Health Information Community (AHIC) in 2005. While privacy was not an initial focus, the Community quickly identified the need to address confidentiality issues in their efforts, and a workgroup on Confidentiality, Privacy, and Security was formed. This group has addressed some areas of identity proofing and the need to protect PHI wherever it might reside, but it also has indicated that there are many more efforts needed including the authentication of individuals involved in health information.

As the Community has addressed standards, and the need for confidentiality, it has also made recommendations for how standards may be affected by privacy and the need for certification of health information technology products that include basic security to facilitate confidentiality. As a result of this effort, the Health Information Technology Standards Panel (HITSP) is looking at confidentiality and privacy standards, and the Commission for Certification of Health Information Technology (CCHIT) is looking to establish certification criteria to identify technology that meets the principles established by the Community and HHS.

As noted, the HHS National Committee on Vital and Health Statistics (NCVHS) has had health information confidentiality as a focus ever since NCVHS was designated as the advisory committee to oversee HIPAA. In recent years the NCHVS Privacy and Confidentiality Subcommittee has concentrated on post-HIPAA privacy and security issues as well as confidentiality as it applies to a nationwide health information network and personal health records. While AHIMA does not support all the recommendations of the NCVHS, we have been very pleased with the work and testimony that the committee has undertaken, and as noted we specifically would point out their efforts on HIPAA versus FERPA.

As members of the committee are aware, the House has passed legislation related to nondiscrimination on the basis of genetic information (HR 493, the "Genetic Information Nondiscrimination Act"). This legislation is now on "hold" in the Senate. As I have noted, AHIMA believes that nondiscrimination should apply to all health information, not just genetic and we would hope that Congress would consider such an approach.

Our members, especially those who fill the role of privacy officers (required by HIPAA) are noting that the issue of privacy for them is moving beyond just healthcare. With the banking and finance

industries becoming more involved in privacy we see that we must soon address the protection of an individual's information uniformly whether it is financial or healthcare. This is an issue that Congress will need to follow as we see more movement and change in healthcare.

As I have mentioned, we also see a need for consumer education. Education needs to address confidentiality and security as well as health information technology and the new environment. It is only with consumer trust that we can build a national infrastructure and adopt or modify laws to facilitate such an exchange.

I have also alluded to that fact that AHIMA and its members are very involved in the area of confidentiality and security. Many of our members are involved in efforts surrounding the PHR, HIE, and protections for health records whether they are paper, electronic, or hybrid form. While it would be wonderful to see one concerted effort, we know from experience that there is a tremendous amount of work that needs to be done because of our federal foundation and approach to legislation and regulation, as well as the evolution that is going on in health information technology and management.

Expansion of Privacy Protection for PHRs

AHIMA has long called for consumer-based personal health records in addition to provider-based electronic health records. This goes back even before the creation of jump-drives and web-based portals. It has been our contention that consumers should have a copy of their medical record, track their current health status, and have an overall healthcare awareness. We have never endorsed a method or a PHR product. We have just endorsed that consumers should use a PHR—whether in paper or electronic form.

To spread the word on the importance of PHRs, AHIMA embarked upon a consumer-education campaign. This campaign combined the use of a consumer web site, www.myPHR.com, with nationwide public speaking engagements by AHIMA members in each and every state.

The web site is a tool that helps visitors some important questions about personal health records:

- Why start a PHR?
- What should your PHR contain?
- What are the steps to be taken to create a PHR?
- Are there different ways to keep your PHR?

In addition, the site provides a free health record form that will help consumers start their own PHRs.

As our public-education campaign continues, so do personal health record developments. Although there is no single model of a personal health record, there are some important concepts that should apply to any PHR.

Today, AHIMA and others in the industry are working hard on interoperable and data standards that will ensure that any electronic PHR is capable of being interoperable with the standard EHR and other electronic records. Currently, AHIMA is leading an effort to ensure the interoperability of the PHR with the Health Level Seven (HL7) standard electronic health record. We expect to see

a new HL7 standard in the not too distant future. AHIMA defines the PHR as "...an electronic, universally available, lifelong resource of health information needed by individuals to make health decisions. Individuals own and manage the information in the PHR, which comes from healthcare providers and the individual. The PHR is maintained in a secure and private environment, with the individual determining rights of access. The PHR is separate from and does not replace the legal record of any provider."

As I indicated, AHIMA believes that protection should follow the personal health information no matter where it might be stored or transferred. This clearly extends to PHRs, which can be stored or offered by a variety of different vendors or operators. Some of these vendors are covered by HIPAA, because they have some healthcare claims function that has made them a HIPAA-covered entity. A few vendors may be covered by state law, but it must be noted that neither HIPAA nor most state laws considered PHRs. The industry is moving that quickly.

Clearly today, PHRs offered by non-HIPAA-covered entities have no protection unless there is state legislation that specifically addresses the issue. Even if state legislation exists, there is concern if the PHR operator is in one state, and the consumer is in another, which law applies and/or prevails. In line with consumer concerns related to discrimination and misuse of personal health information, we recommend that uniform laws be written to cover the misuse of personal health information regardless of where it resides or is transmitted – this would then include the personal health record.

A concern with the information in a PHR relates to who has access and can use the information beyond the individual. As I noted, there are a variety of models of PHRs offered HIPAA covered entities and others. The question is what access and responsibilities should govern the operator or vendor of the PHR. Some health plans have indicated that they have the right to access and use PHRs they operate under the "Treatment, Payment, and Healthcare Operations (TPO) of HIPAA. We think such access for a PHR should be questioned. The first word in PHR is "personal" and it makes sense that the individual provide an additional authorization for any access or use of this PHR record set outside of the individual's own use. If the individual cannot control the access and use to their own PHR, their ability to trust and ensure the appropriate use of their personal information will be eroded. This is especially true when the PHR is in the hands of a third party where there is a concern about potential misuse or discrimination.

Our recommendation, therefore, not only extends to protection against the discrimination and misuse of PHR information, but also for establishing a requirement that any access or use be governed by a separate authorization unless otherwise required by law. In addition, except for PHRs offered by healthcare providers, we believe that individuals (in this case usually subscribers or employees) should be given the right to opt-out of a PHR being built for them or their affected family members. This would mean that no PHR would be populated even with claims data.

While we have some concerns for how some PHRs are populated with claims data, we are pleased to see healthcare providers, health plans, employers, and other types of organizations take steps to make such records available for individuals and for healthcare providers when such data is needed. Even so, the consumer must be fully aware of how the record is populated and how it can be accessed and used. Not only used by themselves, but by their healthcare providers and by the operators of the PHR. If

awareness is not a component, PHRs will fall into misuse, which itself could endanger the health of the individual.

Difference Between Business Associates and 3rd Party Non-Covered Entities

The privacy officer members of AHIMA have often cited the business associate requirement as one of the more difficult aspects of HIPAA to manage. This is especially true when you have a small provider contracted with a very large subcontractor who sets the tone of the relationship. Business associates in the realms of privacy would be subcontractors of HIPAA covered entities, which, as I have already noted, are not all the parties that could be involved with personal health information. Under HIPAA, the covered entity would identify the HIPAA responsibilities to the subcontractor or business associate and the business associate would then be responsible for compliance. If a HIPAA entity discovered that a business associate was not in compliance with HIPAA then it would take corrective action or cancel the contract. The contracts also become difficult to manage when the covered entity's subcontractor itself subcontracts out to complete the work requirements in the contract. As we have seen in some cases, this subcontractor list can extend to multiple parties.

Once again, situations such as these show the need for the confidentiality and security protections to follow the data no matter where it resides or is transferred. The entity holding the identifiable personal health information should be responsible for its safekeeping. The Confidentiality, Privacy, and Security (CPS) Workgroup of the HHS advisory body AHIC last week made a similar recommendation to the Secretary. The CPS recommended:

- *"All persons and entities, excluding consumers, that participate directly in, or comprise, an electronic health information exchange network, through which individually identifiable health information is stored, compiled, transmitted, modified, or accessed should be required to meet enforceable privacy and security criteria at least equivalent to any relevant HIPAA requirements (45 CFR Parts 160 and 164)."*

- *"Furthermore, any person or entity that functions as a Business Associate (as described in 45 CFR §160.103) and participates directly in, or comprises, an electronic health information exchange network should be required to meet enforceable privacy and security criteria at least equivalent to any relevant HIPAA requirements, independent of those established by contractual arrangements (such as a* Business Associate Agreement *as provided for in HIPAA)."*

AHIMA's immediate past president, Jill Callahan Dennis, JD, RHIA, is a member of the CPS workgroup and we believe these recommendations make a lot of sense. The world is far too complicated to be able to use a "business associate" approach especially when we are discussing electronic health exchange among a variety of different entities. Again, let the protections follow the data, and make all parties responsible for confidentiality.

Employer Requests for Information

Another important issue in the current personal health information landscape concerns employer requests for health information. If you have seen some of the consumer polls, you know that consumers have indicated less concern for where their health information resides. Why? Consumers

want their health information to benefit themselves, their families, and their communities. However, what the polls have consistently showed is that consumers fear that their information may used against them for discriminatory purposes by their employer, potential employer, and/or insurers. Eliminating this fear of discrimination is crucial to creating trust in our system and with moving forward with electronic health information exchange. If we can secure data and create trust then we will have an easier time having the data available for a variety of important population health needs as quality measurement, public health surveillance, biosurveillance, and health research.

There are legitimate needs for employers to have some health information about their employees or potential employees, just as there are a few reasons why some insurers need some health information concerning their insured or potential insured. In this instance, I am talking about access to information outside of the claims process. We, and I think this is a government role, need to define the misuse of data and the legitimate reasons for why an employer might require access to personal health information or request information from an employee or potential employee. It is important to define what constitutes health information discrimination versus the legitimate needs for information. Then, if discrimination exists, it should be punished.

It is the government's role to establish a means of punishing those who discriminate or misuse data. Misuse could be the intentional and unwarranted access to, use of, or distribution of an individual's personal health information. There are some laws on the books, including those passed by Congress in 1997, but there have been very few prosecutions. If the public begins to see that the healthcare industry and government are active in this area, it will likely create a greater trust in the system by showing the public that misuse of data has serious ramifications.

Strong "misuse of PHI rules" would also allow the industry and government to prosecute the intention breeches of information that we have seen reported in the media. I do not mean to suggest that all of the potential breeches are intentional or result in a loss of protection. But our industry does need to be held accountable for the security of health information and let us send a message to anyone who desires to breech the confidentiality of healthcare information that they will be punished. Let the protection follow the data and let's punish those who misuse healthcare data or discriminate on the basis of healthcare data. If we do not, consumers will not have trust in our development of EHRs, our establishment of EHI, and access to secondary health information that will better society.

Student Protections

Another important area of consideration is protecting the healthcare data of students. Student healthcare data has two masters, the HIPAA privacy rule and FERPA. Over the past several years, the NCVHS Subcommittee on Confidentiality and Privacy has held several hearings that have highlighted the problems created by having these two laws overlap.

Gone is the day when the school nurse took your temperature and put you on a cot until it was time to go home. Today's school nurses are dealing with students on a variety of drug regimens, some even sporting infusion pumps. Disease outbreaks require that school districts have immunization records. The schools and their nurses should not have to beg parents and family physicians for records. High school coaches need to have a clear and accurate health picture of the players on their teams to take precautions against the child with a heart condition collapsing on the field. It is a difficult balance.

Even though this information is needed to protect against disaster, it should not be available to everyone in the school or in the locker room. FERPA was not designed to provide the protections that Congress and the states have seen as necessary for health information.

Administration of both rules becomes even more difficult for schools such as Vanderbilt. The rules reside side-by-side. Again, we owe it to our citizens to protect the confidentiality of their health information. We suggest that the Congress look at the testimony and recommendations made by the NCVHS with regard to FERPA and HIPAA issues and seek to extend, at a minimum, HIPAA protections to all healthcare data, so there is no question on which of the two laws prevails when discussing healthcare data.

Conclusion

Currently the transformation in healthcare is occurring at a pace unheard of in the industry, and yet some would say it should move even faster. The transformation in healthcare is not just converting healthcare data from paper to electronic, but it is also transforming the business processes and uses of information required in such a metamorphosis. In addition to this conversion we have even more consumer involvement, and rightly so, calling for rigid confidentiality and security assurances that will protect individuals against discrimination and the misuse of their healthcare information. That's a big order, and as I have alluded to this transformation and culture changes it is not happening overnight, but rather will take many years. In the meantime we now find ourselves in the midst of change and in an environment that is neither all paper nor electronic. We also find ourselves in an environment never anticipated by a myriad of existing federal and state laws and regulations that impact our abilities to make the conversion and preserve the needed confidentiality and security practices we have addressed this afternoon.

The industry is in a major transition where different health information exchange models are being discussed for a multitude of environments. While we might desire a simple answer as soon as possible, this will not be the case. Once again, we must suggest that the healthcare industry and government provide protections that will permit a variety of models and the time to approach more specific rules and regulation. As we move forward we must insure that personal health information is protected wherever it might reside. We must insure that individuals are protected against the misuse of their health information for discriminatory and other nefarious purposes. And finally, we must insure that individuals continue to have a right to access to their own healthcare information

In addition to our efforts to make laws, regulations, and practices standard, there is similarly a need to address just how health information technology impacts concerns for privacy. We in the HIM profession believe that new information technology will permit even better security and confidentiality, if the principles and processes surrounding such technology are applied intelligently. But, we have a major need for educating and an understanding of EHRs, PHRs, information exchange.

History has shown that there is no silver bullet that will solve everything but while goals and objectives and even principles can be stated, a detailed map of milestones is very difficult to achieve in our system of government and under our healthcare model. I can assure the committee that many are working on this effort and our goals are becoming more uniform as we move forward.

Over the years, some in Congress have made consistent efforts to legislate in the privacy area. It has been a difficult undertaking to say the least. As the AHIC, NCVHS and others discuss and provide recommendations in the privacy and security area, Congress can also begin to look at some very important issues:

- The need to insure that confidentiality protections follow the information no matter where it resides or is transferred.
- Comprehensive nondiscrimination legislation that has harsh penalties for the misuse and illegal requests for health information.
- The need to prosecute those who break the law.
- The need to penalize those entities whose confidentiality and security processes and technologies do not comply with the level of confidentiality protection required by law.
- The need to eliminate the conflicts between HIPAA v FERPA.
- Conscientious review of proposed laws to identify barriers that may arise that would impede deployment of health information technology products, expansion of health information exchange, and critical uses of health information—as for quality reporting, biosurveillance, and public health.

Mr. Chairman and members of the subcommittee, I hope that my testimony has given you an insight into the aspects of healthcare confidentiality and security that you are seeking and that my recommendation will provide you with guidance as you address the many thorny questions facing our community. I stand ready to answer any further questions or concerns you might have, and as president of AHIMA, I similarly make available to you the resources of our staff to assist in any way possible.

Contact information.

Bryon Pickard, MBA, RHIA
Director of Operations
Vanderbilt Medical Group
2146 Belcourt Avenue
Nashville, TN 37212
(615) 936-2000

Don Asmonga, MBA
Director of Government Relations
AHIMA
1730 M Street, NW, Suite 502
Washington, DC 20036
(202) 659-9440

Dan Rode, MBA, FHFMA
VP, Policy & Government Relations
AHIMA
1730 M Street, NW, Suite 502
Washington, DC 20036
(202) 659-9440

Craig May
Director of Public Relations
AHIMA
233 North Michigan Avenue
21st Floor
Chicago, IL 60601
(312) 233-1100

Statement on Health Information Confidentiality
A Joint Position Statement
by
American Medical Informatics Association
American Health Information Management Association
July 2006

The American Medical Informatics Association (AMIA) and the American Health Information Management Association (AHIMA) have a long history of working to protect the confidentiality of individuals' health information and to promote fair information practices. Public confidence that privacy will be protected and that identifiable information will be used only for purposes authorized by the individual, or otherwise permitted by law are essential to ensuring trust in a nationwide health information network (NHIN that facilitates sharing of personal health information (PHI). As the United States progresses from a paper-based system of health records to an electronic environment, AMIA and AHIMA believe that the following principles should be incorporated in all rules, regulations, or laws pertaining to PHI.

Any organization that accesses or stores PHI should abide by the following principles. The organization should:

- Inform individuals, through clear communications, about their rights and obligations and the laws and regulations governing protection and use of PHI.
- Notify individuals in clear language about the organization's privacy practices and their rights in cases of breaches
- Provide individuals with a convenient, affordable mechanism to inspect, copy, or amend their identified health information/records
- Protect the confidentiality of PHI to the fullest extent prescribed under HIPAA, regardless of whether the organization is a "covered entity" as defined in HIPAA, and ensure that the organization and its employees all comply with HIPAA, state laws, and the policies and procedures put in place to protect PHI.
- Use PHI only for legitimate purposes as defined under HIPAA or applicable laws.
- Prohibit the use of PHI for discriminatory practices, including those related to insurance coverage or employment decisions
- Timely notification of individuals if security breaches have compromised the confidentiality of their personal health information.
- Work with appropriate law enforcement to prosecute to the maximum extent allowable by law any individual or organization who intentionally misuses PHI
- Continue to improve processes, procedures, education, and technology so that PHI practices improve over time.

Furthermore, because PHI is expected to flow across organizational boundaries through the NHIN, it is important that the following principles covering information when it is transferred from one entity to another also apply:

- Health information privacy protections must follow PHI no matter where it resides

- Uniform and universal protections for PHI should apply across all jurisdictions in order to facilitate consistent understanding by those covered by such laws and the individuals whose health information is covered by such laws.

About AMIA
The American Medical Informatics Association (AMIA) is an organization of 3,500 health professionals committed to informatics who are leaders shaping the future of health information technology and its application in the United States and 41 other nations. AMIA is dedicated to the development and application of informatics in support of patient care, teaching, research, and health care administration and public policy. www.amia.org

About AHIMA
The American Health Information Management Association (AHIMA) is the premier association of health information management (HIM) professionals. AHIMA's 50,000 members are dedicated to the effective management of personal health information needed to deliver quality health care to the public. Founded in 1928 to improve the quality of medical records, AHIMA is committed to advancing the HIM profession in an increasingly electronic and global environment through leadership in advocacy, education, certification, and lifelong learning. www.ahima.org

7-31-2006

The Value of Personal Health Records
A Joint Position Statement for Consumers of Health Care
by
American Health Information Management Association
American Medical Informatics Association
February 2007

Position
The American Health Information Management Association (AHIMA) and the American Medical Informatics Association (AMIA) advocate empowering individuals to manage their healthcare through the use of a personal health record (PHR). The PHR is a tool for collecting, tracking and sharing important, up-to-date information about an individual's health or the health of someone in their care. Using a PHR will help people make better health decisions and improves quality of care by allowing them to access and use information needed to communicate effectively with others about their healthcare.

Basic Principles
- Every person is ultimately responsible for making decisions about his or her health.
- Every person should have access to his or her complete health information. Ideally it should be consolidated in a comprehensive record.
- Information in the PHR should be understandable to the individual.
- Information in the PHR should be accurate, reliable, and complete.
- Integration of PHRs with EHRs of providers allows data and secure communication to be shared between a consumer and his or her health care team.
- Every person should have control over how their PHR information is accessed, used and disclosed. All secondary uses of PHR data must be disclosed to the consumer, with an option to opt-out, except as required by law.
- PHR products should be certified by CCHIT to comply with data standards, include a minimum data set, identify each data's source, and meet security criteria consistent with HIPAA
- The operator[1] of a PHR must be accountable to the individual for unauthorized use or disclosure of personal health information. The consumers should be notified immediately of breeches in security that could lead to disclosure of personal health information.
- A PHR may be separate from and does not normally replace the legal medical record of any provider.
- Privacy protection of PHR data should follow the data. PHR data must not be used in any discriminatory practices.

[1] An "operator" could be a healthcare provider, health plan, commercial supplier, government agency, employer, union, fraternal order, and so forth.

Questions and Answers

Why should everyone have a PHR? We believe that all individuals should be able to readily access, understand, and use their personal health information. A PHR allows individuals to be more active partners in their healthcare, and gives them up-to-date information when and where they need it. A PHR provides a single, detailed and comprehensive profile of a person's health status and healthcare activity. It facilitates informed decisions about the care of the individual. It may also reduce duplicate procedures or processes – such as repeated lab tests and x-rays – saving time and money. A PHR helps people prepare for appointments, facilitates care in emergency situations, and helps track health changes.

What media should you use for a PHR? We encourage individuals to begin tracking their health information in whatever format works best for them, even if the choice is paper. We recommend that individuals use an electronic media to facilitate a timely, accurate, and secure exchange of information across healthcare institutions and providers. PHR information should always be stored in a secure manner just as you would store other confidential personal information such as financial information.

How can an individual choose a PHR supplier? Individuals can create their own PHR, or may be offered one by a variety of sources, such as a healthcare provider, insurer, employer or a commercial supplier of PHRs. Each supplier has different policies and practices regarding how they may use data they store for the individual. Study the policies and procedures carefully to make sure you understand how your personal health information will be used and protected. Policies to look for include privacy and security; the ability of the individual, or those they authorize, to access their information; and control over accessibility by others. If the PHR contains the same information that the doctor has seen, it has more usefulness for tracking purposes than information from insurance forms. For example, insurance claims information may list the diagnosis or medication but not the details (for example, actual blood pressure reading or dose of the medication taken).

What should a PHR contain? Broader than a medical record, the PHR should contain any information relevant to an individual's health. In addition to medical information such as test results and treatments, a PHR may include diet and exercise logs or a list of over-the-counter medications. A PHR should contain the following information:

- Personal identification, including name and birth date
- People to contact in case of emergency
- Names, addresses, and phone numbers of your physicians, dentists, and specialists
- Health insurance information
- Living wills, advance directives, or medical power of attorney
- Organ donor authorization
- A list and dates of significant illnesses and surgical procedures
- Current medications and dosages
- Immunizations and their dates
- Allergies or sensitivities to drugs or materials, such as latex
- Important events, dates, and hereditary conditions in your family history
- Results from a recent physical examination
- Opinions of specialists
- Important tests results; eye and dental records
- Correspondence between an individual and his or her provider(s)
- Current educational materials (or appropriate web links) relating to one's health

Where individuals should begin: A good place to begin is with a visit to www.myPHR.com (a site provided as a free public service by AHIMA) for further information on creating and managing a PHR. We suggest that people find out if their healthcare providers, employer, insurers, or another individual or organization offers a PHR. If an individual needs to obtain copies of medical records themselves, they can contact doctors' offices or each facility where they have received treatment.

Each person can create a PHR at his or her own pace, perhaps starting with the next medical visit. The important thing is to get started.

Note: Because the use of personal health records is an issue of importance to both organizations, AHIMA and AMIA collaborated on the development of this joint position statement.

About AHIMA
The American Health Information Management Association (AHIMA) is the premier association of health information management (HIM) professionals. AHIMA's 50,000 members are dedicated to the effective management of personal health information needed to deliver quality health care to the public. Founded in 1928 to improve the quality of medical records, AHIMA is committed to advancing the HIM profession in an increasingly electronic and global environment through leadership in advocacy, education, certification, and lifelong learning. www.ahima.org

About AMIA
The American Medical Informatics Association (AMIA) is an organization of 3,500 health professionals committed to informatics who are leaders shaping the future of health information technology and its application in the United States and 41 other nations. AMIA is dedicated to the development and application of informatics in support of patient care, teaching, research, and health care administration and public policy. www.amia.org

2-1-2007

Foundation of Research and Education/AHIMA Sponsored Programs, Research Contracts and Grants* January 1, 2006 to April 23, 2007			
A. Active Projects 2007; B. Proposals Pending 2007; C. Projects Funded and Completed 2006 and 2007; D. Proposals without Funding, Rejected, or on Hold for Other Reasons			
A. Active Projects 2007			
Federal Contract	ONC—State Level Health Information Exchange Consensus Project	Office of the National Coordinator (ONC)	Primary Staff Involvement: Sue Fiorio, Aleta Harris, Linda Kloss, Eileen Murray, Carol Nielsen, Theresa Reynolds
The purpose of this contract is to build on and extend the work produced to date by the Foundation of Research and Education (FORE) on emerging best practices and guidance for state level health information exchange initiatives (HIEs). These organizations are evolving very rapidly and the lessons learned must be documented, studied, and made available to all state level entities and other interested stakeholders. This contract will produce research-based technical work products to expand the body of knowledge of emerging best practices. It is expected that these will help not only state level HIE initiatives, but also regional health information exchange initiatives, state governmental e-Health programs and others who are working to advance care transformation through health information.			
Value of Total Contract: $793,785.00			
Federal Professional Services Contract	#200-2006-M-18081: Training for Coders for Morbidity and Mortality: ICD-10 Curricula	CDC: National Center for Health Statistics	Primary Staff Involvement: Kathy Giannangelo
This project involves implementing, piloting, and evaluating the first phase of the International Training and Certification Program for ICD-10 Mortality and Morbidity Coders. The purpose of the project is to expand on the work already accomplished by the Joint Collaboration to pilot the processes for testing and certification of practicing ICD coders and newly trained coders and for the recognition of ICD trainers and educators and to evaluate the strengths and weaknesses of the processes. The project also will perform outreach to coders and trainers in order to inform them of the availability and benefits of the international program.			
Value of Total Contract: $20,000			
Subcontract from RTI for Professional Services Funding Primary Source is AHRQ	Contract to Develop Model Anti-Fraud Requirements for Electronic Health Records	HHS/AHRQ	Primary Staff Involvement: Michelle Dougherty, Don Mon, Harry Rhodes
The RTI research team has previous experience identifying fraudulent or otherwise suspicious activity in large datasets and recommends an iterative two-pronged approach for this task, which includes the use of scoring algorithms and anomaly detection. Known patterns of fraudulent behavior can be characterized and modeled using supervised learning or rule induction models. The resulting scoring algorithms can be used to screen transactions for potentially fraudulent or otherwise suspicious activity. Unsupervised learning strategies, on the other hand, can be used to identify unusual or anomalous activity worthy of additional review and follow-up. Fraudulent behavior identified through the use of anomaly detection can then be modeled and added to the array of scoring algorithms used to screen additional data for patterns suggestive of fraud or other suspicious activity.			
Value of Total Contract: $115,326.00			
Contract	Center for Aging Services Technology: Development of a Framework for Continuity of Care Document (CCD) Functional Status and Wellness Content	Center for Aging Services Technology—a program of the American Association of	Primary Staff Involvement: Jill Burrington-Brown, Rita Scichilone

	RE ID #: 35501	Homes and Services for the Aging	

AHIMA will assist in the establishment of stakeholder work groups to advance health information technology and terminology standards related to functional status assessment and advocacy for electronic health record use for wellness measurement and consumer empowerment through the use of personal health records.

Value of Total Contract: $54,600.00

Service Contract	SNOMED:ICD-9-CM Map Validation Process – Phase II	National Library of Medicine	Primary Staff Involvement: Jill Bonnart, Susan Fenton, Kathy Giannangelo, Karen Kostick, Rita Scichilone

Note: this project is funded but the actual task is still in the proposal phase. This is a draft of the tasks that were submitted. The goal of this phase of the map validation project is to produce small subsets of the SNOMED:ICD-9-CM reimbursement use case map in a timely fashion for testing and use by the industry. Given that this is a reimbursement use case map; this phase will focus on the most frequent conditions and diagnoses as determined by the National Center for Health Statistics via their National Hospital Discharge Data Set and National Ambulatory Care Data Set. It is thought that these will be more representative of diagnoses submitted to all payors rather than utilizing CMS data which, of course, is limited to CMS claims.

Value of Total Contract: $13,999.62 carried over from the base year plus $50,000 from Option Year 1--grand total of $63,999.62 for use in Option Year 2.

B. Proposals Pending

Federal Grant	AHRQ—Ambulatory Safety and Quality: Enabling Patient-Centered Care through Health IT: Effects of Patient-Centric Care Management Technology: A Randomized Trial	HHS: AHRQ RFA-HS-07-007	FORE Subcontract: Jill Burrington-Brown, Susan Fenton, Carol Nielsen

Letter of Intent: January 19, 2007; Proposal February 15 Prime: Univ. of Central Florida, Dr. Thomas Wan, PI
The proposed research focuses on a demonstration of patient-centric care technology to improve medication management, utilizing the PHR as a facilitator for improved patient-provider communication. The patient-centric care technology demonstration project will assess and address the use of PHR health Information Technology (IT) as a facilitator for improving ambulatory patient safety and quality, identify the systemic barriers to health IT adoption for older, minority and underserved populations, improving patient health outcomes and asses patient–clinician satisfaction. Additionally, the PHR is a vehicle for developing a process for obtaining and documenting a complete list of current patient medications at each office visit, reducing medication errors by deescalating Adverse Drug Events (ADE) and Sentinel Events(SE) from medications, improving perceptions of patient-clinician communication, and measuring healthcare outcomes, specifically inappropriate use of healthcare resources.

Totals	Yr. 1 $50, 745.00	Yr. 2 $19,221.00	Yrs. 3 $24,743.00	Total Direct & IDC over 3 years

Federal Grant	AHRQ—Ambulatory Safety and Quality: Enabling Patient-Centered Care through Health IT: Performance Measure Variation: Data Elements, Collection, and Outcomes	RFA-HS-07-002	Susan Fenton, Crystal Kallem, Eileen Murray, Carol Nielsen

Letter of Intent: January 19, 2007	Submitted on 2/14/2007	Anticipated Star Date: July, 2007	Prime: Dr. Jennifer Garvin, VA Philadelphia

Contract	Consultation on key questions concerning the	Language and Computing	Primary Staff Involvement: Rita Scichilone

	E&M rules and review of possible interpretations.		

Language and Computing (L&C) is building a coding for billing NLP application that initially focuses on E&M coding. As part of the process, L&C must ensure that it follows applicable rules according to widely accepted interpretations. Interpretation of rules is a major variable for two reasons. First, the rules published by the payors, including Medicare, are extremely imprecise. Second, there are intermediates in the payment process called "carriers" for each region of the country that are responsible for implementation. These "carriers" are able to apply their own interpretations of the rules. The best recourse for a vendor in our situation is to develop a consulting relationship with an organization that has broad knowledge of the issues raised by interpretation of rules. AHIMA is the organization in the best position to help L&C in this manner. Staying abreast of coding issues is one of the roles they play for the provider community. It is a respected organization by both providers and payors. Ultimately, AHIMA will be involved in an independent evaluation of our tools. Thus, they are an ideal source for consulting about interpretation of coding for billing rules.

Value of Total Contract: $9600 depending upon number of hours billed

Federal Grant	AHRQ Small Conference Grant Program: Solutions to Accelerate SNOMED CT ® Implementation in Electronic Health Record Systems	HHS: AHRQ	Primary Staff Involvement: Susan Fenton, Kathy Giannangelo

The Foundation of Research and Education (FORE) of the American Health Information Management Association (AHIMA) will hold a cross industry national conference to identify solutions to expand and accelerate the adoption and implementation of SNOMED CT® in Electronic Health Record (EHR) systems. This conference will convene approximately 125 representatives from various stakeholder organizations who can determine the enablers and barriers to adoption and use of SNOMED CT in the short and long term. The participants will describe the business case for a reference terminology and develop recommendations for an integrated strategy for the use of the SNOMED CT data standard. Participants will contribute to the development of a white paper and other supporting documentation that will describe a nationwide strategy for aligning vendor and end user SNOMED CT implementation efforts so they converge and can serve as a foundation for health information exchange.

Value of Total Grant Application: $46,182.59

C. Projects Completed in 2006 and 2007

Federal Contract	HHSP23320064105 EC: RHIO Develop Consensus Best Practices for State Level Regional Health Information Organizations—Initial Contract March to August, 2006	Office of the National Coordinator (ONC)	Primary Staff Involvement: Linda Kloss, Don Mon, Eileen Murray, Harry Rhodes

The purpose of the project was to gather information from existing state-level RHIOs to determine successful governance, legal, financial and operational characteristics, to develop consensus on guidance for developing state-level HIE initiatives, and to widely disseminate these findings. The research was guided by a Steering Committee of leaders from the state level RHIOs that were studied and a panel of national experts who served as Technical Advisors. They identified these three targeted areas, the interaction with federal activities, financial sustainability through HIE, and the role of payers, as critical areas for further inquiry.

Value of Total Contract: $489,745.00

Subcontract from Research Triangle Institute—Federal Flow-Through	Privacy and Security Solutions for Interoperable Health Information Exchange	HHS/AHRQ	Primary Staff Involvement: Susan Fenton, Don Mon, Harry Rhodes

The American Health Information Management Association (AHIMA) developed an assessment tool evaluating perceived barriers in state laws and business practices that pose interoperability challenges and hinder the free flow of information among all stakeholders involved in interoperable health information exchange and identify "best" practices for overcoming interoperability barriers.

Value of Total Contract: $63,345.00			
Subcontract	National Conference On Health Care Data Collection and Reporting	AHRQ	Primary Staff Involvement: Crystal Kallem, Don Mon, Alison Viola
The Foundation of Research and Education (FORE) of the American Health Information Management Association (AHIMA) and the Medical Group Management Association Center for Research (MGMA CFR) have partnered with the Agency for Healthcare Research and Quality to conduct a national conference on heath care data collection and reporting. This invitational conference will convene approximately 50 persons from various stakeholder organizations that can contribute to the development of a set of recommendations for effectively coordinating various performance measurement initiatives to maximize value and minimize data collection burden and expense for health care providers. Participants will contribute to the development of multiple articles and papers that will describe a national strategy for developing standard methodologies in health care performance measurement, data collection and reporting.			
Value of Total Contract: $21,525.00			
Federal Contract	HHSP23320064105 EC: RHIO Develop Consensus Best Practices for State Level Regional Health Information Organizations—Second Extension	Office of the National Coordinator (ONC)	Primary Staff Involvement: Crystal Kallem, Linda Kloss, Don Mon, Eileen Murray, Harry Rhodes
This project will study three specific aspects of the operation of state-level Regional Health Information Organizations (RHIOs): their interaction with federal activities for health care and information technology, health information exchange (HIE) projects that have achieved financial sustainability and the role of public payers on state-level HIE.			
Value of Total Contract: $199,890.00			
Federal Contract	HHSP23320064105 EC: RHIO Develop Consensus Best Practices for State Level Regional Health Information Organizations—Third Extension	Office of the National Coordinator (ONC)	Primary Staff Involvement: Linda Kloss, Eileen Murray
The purpose of this contract extension is to establish and support a dynamic process for continuing to build the body of knowledge about the best practices of state-level health information exchange (HIE) initiatives. This contract extension will put in place the structure and processes to study and document best industry practices as they continue to evolve in these and other organizations. In this way, the *Workbook* and related resource materials will be a dynamic reflection of dynamic organizations. The specific goals are as follows: • Track the evolving practices of selected HIE organizations in the areas of governance, financing, health information exchange, and technology and incorporate these into an up to date *Workbook*. • Host quarterly roundtables to seek input to strategic issues that reflect barriers or opportunities, changing market conditions, or new lessons learned and prepare reports of these deliberations. • Capture characteristics and competencies of the evolving models for state-level HIEs • Ensure that findings are communicated to all interested state-level HIE organizations and are available through the AHRQ HIT Resource Center, to the NGA State Alliance for e-Health, the National Conference of State Legislatures and to other public domain resource centers working to advance health IT. • Serve as a point of contact to represent the state-level HIE perspective			

Value of Total Contract: $139,958.63

Mr. CLAY. Thank you so much, Mr. Pickard.
Mr. Swire, of the Ohio State University.

STATEMENT OF PETER SWIRE

Mr. SWIRE. The Ohio State University, home of the Buckeyes. Yes, sir.
Mr. CLAY. Yes, sir.
Mr. SWIRE. Mr. Chairman, members of the subcommittee, thank you very much for the invitation to testify here today on privacy and security of electronic health records.
Today fewer than 10 percent of our clinical records in the country are accessible in electronic form, and all of us hope that number climbs sharply in the next decade.
My colleague at the Center for American Progress, Karen Davenport, has recently released a new report about health IT and the quality improvements, and, Mr. Chairman, I ask if that could be submitted to the record for this hearing.
Mr. CLAY. Yes, please.
Mr. SWIRE. Thank you.
To make this shift to the NHIN, the National Health Information Network, we need to get privacy and security right. Public surveys repeatedly showed that these privacy concerns are top of mind when it comes to the shift to electronic health records. Unless Americans are convinced that effective safeguards are in place, many of the benefits of this NHIN may be delayed or lost entirely.
My written statement addresses various issues, but I would highlight two things in the testimony today: preemption and enforcement.
On preemption, my theme is that the wrong sort of preemption would actually repeal many existing privacy and security safeguards. On enforcement, the current no enforcement system is not a sound basis for going forward with electronic health records.
Briefly, my background before returning to law teaching, I served as chief counselor for privacy in the U.S. Office of Management and Budget in 1999 and 2000, and in that role I was the White House coordinator for the HIPAA privacy rule. This has lost me many friends in the medical community.
During that time we had over 50,000 public comments on the proposed rule, and I co-chaired the process to look at those, try to respond to them, and come up with a final rule by the end of 2000, and I have worked in this area since. So it is based on that I try to offer some observations today.
On preemption, my first theme is that simple preemption of State laws going to HIPAA alone would repeal many existing privacy protections.
In many States we have protections for things like HIV records, mental health, substance abuse, reproductive records, Public Health Agency records, genetic records, and if we simply say let's do HIPAA, then that means that all of the State protections would be repealed.
In Ms. Grealy's testimony, they feature Indiana as a State to look to. Indiana has the fewest State safeguards, and so harmonizing on that level would be a drop in privacy protection, and we should be careful about doing that.

On enforcement, I have serious concerns about the lack of enforcement from HHS. This is an oversight issue. This creates an obstacle to going forward with electronic health records. If no enforcements are brought under the current system so far under HIPAA, why should the public trust we are going to have good enforcement for the next generation?

Let me emphasize my criticism here goes to law and policy and not to the good faith or the intelligence or hard work of people at HHS, but there are some legal problems the Congress may need to address.

There are three principal problems in enforcement:

First, the batting average for HHS is pretty low. There has been 27,000 complaints and zero civil or monetary penalties, so over 27,000. That doesn't create a lot of confidence.

Second, the current administration has adopted the policy of one free violation. In an enforcement rule last year, HHS said that the first violation simply won't lead to a penalty; instead, it will lead to a planned correct going forward. This sends the signal that medical privacy shouldn't be taken seriously. If you are a covered entity, just wait until they come the first time and then you can fix it, but you don't face any exposure.

Third, the Department of Justice has dropped the ball on criminal prosecution. Justice has received almost 400 referrals from HHS and has brought zero cases under those 400 referrals. These are the most serious cases, and the problem is that, once it goes to DOJ, under current policy HHS stops all proceedings, so the most serious cases HHS doesn't do it and DOJ doesn't do it.

This lack of enforcement has been the subject of major stories in the Wall Street Journal and the Washington Post. One expert was quoted in the post saying, "HHS really isn't doing anything, so why should I worry?"

The lack of HIPAA enforcement will make it harder to build the next generation of electronic health records. Critics will be on strong and legitimate ground saying they can't trust the current system, much less the higher level of trust we would want to have if we go to the all-electronic NHIN.

In my testimony I point out that we can respond to these problems perhaps by HHS changes or by targeted legislation. Here are three things to consider, and then I will close: first, HHS can end the one free violation part of the enforcement reg; second, we should end the current interpretation where HHS stops its own enforcement efforts in the most serious cases whenever there is a criminal referral to DOJ; and, third, a mistaken Department of Justice legal opinion that narrowed the criminal provisions of HIPAA should be revisited. They really take the position that only the hospital that intentionally violates the law and not any of the individuals who break the law can be enforced.

That concludes my comments. I welcome any questions you may have.

[The prepared statement of Mr. Swire follows:]

Center for American Progress

STATEMENT OF PROFESSOR PETER P. SWIRE
C. WILLIAM O'NEILL PROFESSOR OF LAW
MORITZ COLLEGE OF LAW, THE OHIO STATE UNIVERSITY
SENIOR FELLOW, CENTER FOR AMERICAN PROGRESS

BEFORE

THE U.S. HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM, SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES

ON

THE PRIVACY AND SECURITY OF ELECTRONIC HEALTH RECORDS

JUNE 19, 2007

Mr. Chairman, Mr. Ranking Member, members of the Committee:

Thank you for your invitation to testify today on the privacy and security of electronic health records. Our medical system is now striving to move toward what is often called the National Health Information Network. Today, less than 10 percent of our clinical records are accessible in electronic form. All of us hope that that number climbs sharply in the next decade. As my colleague Karen Davenport has stressed in a new report, improved health information technology is essential to improving the quality of our nation's health care.[1]

To make the shift to the NHIN, we need to get privacy and security right. Public surveys repeatedly show that privacy and security concerns are top-of-mind when it comes to the shift to electronic health records. Unless Americans are convinced that effective safeguards are in place, then many of the benefits of the NHIN may be delayed or lost entirely.

My testimony today highlights two key issues—preemption and enforcement.

First, preemption of state laws would effectively repeal many existing privacy and security protections. There is a national baseline of protection under the Health Insurance Portability and Accountability Act of 1996. The HIPAA privacy and security rules, on which I worked extensively, offer essential safeguards for patient records. They are incomplete, however. It is the states that provide the current protections for sensitive records such as mental health, HIV, genetic information, and other key categories of records. The NHIN should be an occasion for strengthening safeguards, and not repealing numerous safeguards in the name of federal preemption.

Second, the current "no-enforcement" system is not a credible basis for EHRs and the NHIN. HHS has received over 27,000 HIPAA privacy complaints but has yet to bring its first case for civil monetary penalties. HHS has needlessly adopted a "one free violation" policy, guaranteeing covered entities that they can violate the law the first time without financial punishment. And the Department of Justice has interpreted the HIPAA criminal provisions in misguided and narrow ways. As explained below, each of these problems can and should be fixed through targeted legislation or regulatory change.

Background

I am the C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University, and a Senior Fellow at the Center for American Progress. I live in the Washington, D.C. area.

From 1999 until early 2001 I served as the Chief Counselor for Privacy in the U.S. Office of Management and Budget. My biggest single project in that role was acting as the White House coordinator for the HIPAA medical privacy rule. Working with HHS, we announced the

[1] Karen Davenport, "Navigating American Health Care: How Information Technology Can Foster Health Care Improvement," Center for American Progress, May, 2007, *available at* http://www.americanprogress.org/issues/2007/06/health_IT_report.html.

proposed rule in October 1999. There were over 52,000 public comments on the proposed rule. The final rule, including responses to all of those comments, was released in December 2000. Shortly thereafter, I returned to my law teaching position. In 2002, HHS announced modifications to the medical privacy rule. The rule went into full effect in April, 2003.

Since leaving government at the beginning of 2001, I have worked extensively on medical privacy and security issues. My CV details my writings and speeches on these issues. From 2004 until 2006 I was a member of the Markle Foundation's Connecting for Health Task Force. Connecting for Health's Common Framework is an outstanding set of materials about how to create private and secure health information exchange. For detailed discussion of security and privacy issues, I commend those papers to the committee's attention.

Since 2001, in compliance with my university's limits on outside consulting, I have also worked on medical privacy and security issues for private-sector clients, as a consultant to the law firm of Morrison & Foerster, LLP. This work with an array of clients has given me hands-on experience in what it is like to comply with the privacy and security rules. None of these clients has paid me in connection with the testimony today, and the views expressed here are entirely my own.

Preemption of State Laws Would Effectively Repeal Many Existing Privacy and Security Protections

My first theme today is that simple preemption of state laws would effectively repeal many existing privacy and security protections.

To understand the preemption issue, it is useful to start with the case in favor of preemption made by in industry. This view starts with a correct factual premise—the benefits of sharing electronic clinical data are high. As Newt Gingrich has often said, "Paper kills." We need to move to a more networked version of health care. The shift to electronic records has occurred in banking, travel, and most other sectors, and it is inevitable and desirable for it to occur for clinical health records.

On all of this I agree. The next part of the pro-preemption position asserts that we can only have a national health information network if we have a national set of rules. HIPAA forms that national baseline, and so we should harmonize on the HIPAA standard. In short, goes this argument, preemption is essential to a national network—it's a "no-brainer."

Although I sympathize with the system designers who struggle with diverse state laws, the effects on privacy and security from this sort of preemption would be large and negative. To see why, it is important to realize that protections for the most sensitive categories of medical information are set forth in state law, and not in HIPAA. Here are some categories of medical records that are often protected at the state level today:

- HIV and other sexually transmitted diseases
- Mental health (beyond the limited scope of "psychotherapy notes" defined in HIPAA)
- Substance abuse and alcohol

- Reproductive and contraceptive care (where states vary widely in policy)
- Records held by public health and other state agencies
- Genetic records

The key thing to realize is that HIPAA simply does not have provisions for these topics. If there is federal preemption on the HIPAA baseline, then there will be a large drop in privacy protection, especially for the most sensitive records.

A related point is that many reporting regimes have been linked closely with privacy protections. To take one important example, extra-strict protections for HIV records have been a package deal with HIV reporting requirements. The concern is that individuals will decide not to get tested unless they are promised strong confidentiality. If we repeal these confidentiality protections, such as through federal preemption, then we will face the public health risks from the spread of communicable diseases.

In the medium term, the lack of preemption is likely to be more manageable than many in industry have assumed. Electronic health records are being deployed in regional health information organizations, and many of those RHIOs cover only one or a few states. A New York City RHIO, for instance, could manage the vast bulk of its records by complying with the laws of New York, New Jersey, and Connecticut. As we build out from these regional systems, each RHIO can share its expertise about relevant state laws with other RHIOs. The path toward compliance with state law is thus far simpler than it would be if we tried to do a massive and instantaneous shift to a 50-state system.

As a final point on preemption, the state laws that are often seen as "burdens" by industry have another name from the consumer perspective—consumer "protections." In light of the strong privacy and security concerns about the NHIN, there should be no rush to repeal these state privacy and security protections.

The Current "No-Enforcement" System Is Not a Credible Basis for EHRs and the NHIN

I have serious concerns about the current enforcement, or lack of enforcement, of HIPAA privacy complaints. This lack of enforcement creates a major obstacle to public acceptance of EHRs and the NHIN—if no enforcement actions are brought under HIPAA, why should the public trust that there will be effective enforcement as far more medical records flow around the NHIN?

Let me emphasize that my criticism here goes to law and policy, and not to the good will or competence of the individuals at HHS who work on enforcement at the Office of Civil Rights. From my time in the government and since, I have been uniformly impressed with the quality of people who have worked on privacy and security issues.

There are three principal problems:

- First, the batting average at OCR is low, to say the least—zero civil penalties for over 27,000 complaints. Through the end of April 2007, OCR reported a total of 27,070

HIPAA privacy complaints, with over 4,500 resolved through investigation or enforcement. Despite this heavy volume, not a single case has yet resulted in civil monetary penalties.

- Second, the current administration has adopted the policy of "one free violation." In the 2006 enforcement rule adopted by HHS, the decision was made that a covered entity would simply not be subject to civil penalty for its first violation.[2] Instead, the first offense always results in a plan to correct actions going forward. This "one free violation" policy sends the signal that medical privacy rules are not taken seriously—a covered entity can be lax in its protection of patient records, secure in the knowledge that it can fix the problems if and when a complaint is filed.

- Third, the Department of Justice has dropped the ball on criminal prosecution. In a 2005 legal opinion that I have criticized previously,[3] the Office of Legal Counsel interpreted the HIPAA criminal provision extremely narrowly. Under this opinion, even the purchase and sale of hospital records, for criminal gain, could not be prosecuted under HIPAA. Although some of those problems have since been solved,[4] main Justice has failed to bring a single indictment on any of the 393 cases that HHS has referred for prosecution. These are the most serious cases that HHS has found, but none of them has yet resulted in criminal indictment or civil monetary penalties.[5] The lack of Justice Department action on these referrals is important, because the Office of Legal Counsel has stated that no civil monetary penalties may be imposed for actions that are punishable under the HIPAA criminal statute.[6]

This lack of enforcement has been the subject of major stories in *The Wall Street Journal* and *The Washington Post*,[7] but HHS and Congress have not responded to date. As *The Washington Post* quoted one medical records specialist, "They are saying, 'HHS really isn't doing anything, so why should I worry?'"

---

[2] Under Section 160.312, the regulation states that "the Secretary *will* [not may] attempt to reach a resolution of the matter satisfactory to the Secretary by informal means." 71 Fed. Reg. 8390, 8425 (Feb. 16, 2006). Under the regulation, civil monetary penalties can be assessed only if no agreement is reached by informal means. I do not believe that this position is required by statute. Whether or not it is currently required by statute, the Congress could decide to change this policy by new legislation.

[3] Peter Swire, "Justice Department Opinion Undermines Medical Privacy," Center for American Progress (2005), *available at* http://www.americanprogress.org/issues/2005/06/b743281.html.

[4] My understanding is that Department of Justice prosecutors in the field have been able to bring some HIPAA prosecutions under an innovative approach described by Assistant U.S. Attorney Peter Winn, "Who is Subject to Criminal Prosecution Under HIPAA?" *Available at* http://www.abanet.org/health/01_interest_groups/01_media/WinnABA_2005-11.pdf.

[5] I understand that five criminal cases have been brought to date by U.S. attorneys acting on evidence uncovered in their districts, and not based on referrals by HHS.

[6] The Office of Legal Counsel opinion, at note 13, quotes 42 U.S.C. § 1320d-5(b)(1) for this conclusion, and reaches the remarkable conclusion that "the Secretary may not impose civil sanctions for the commission of an act that subjects a person to the possibility of criminal prosecution, regardless of whether the person is in fact punished criminally." This position is peculiar, to say the least. It seems to mean that a covered entity would be better off doing a serious violation that is criminal, in order to avoid any possibility of civil sanctions.

[7] Theo Francis, "Medical Dilemma: Spread of Records Stirs Patient Fears Of Privacy Erosion,"*The Wall Street Journal,* Dec. 26, 2006; Rob Stein, "Medical Privacy Law Nets No Fines," *The Washington Post*, June 4, 2006.

I have been at conferences where covered entities themselves, including military hospitals, have asked HHS for more enforcement. These unusual complaints—calls for more enforcement by those subject to enforcement—have been based on their experience that it is too difficult to get resources and management attention for data privacy and security now that the zero-enforcement system is known. These complaints are echoed by a report from the American Health Information Management Association, which found in 2006 that HIPAA compliance had actually fallen compared with previous years, due especially to lack of resources and management attention.[8]

The lack of HIPAA enforcement will make it harder to build the next generation of electronic health records. Critics will be on strong ground in saying they can't trust the integrity of the current system, much less have the level of trust needed for the greatly expanded flow of electronic records in the NHIN.

To respond to these problems, targeted legislation could address the following:

- First, end the "one free violation" part of the enforcement regulation.
- Second, end the current interpretation where HHS stops its own enforcement efforts in the most serious cases, whenever there is a criminal referral to DOJ.
- Third, overrule the Office of Legal Counsel opinion that incorrectly and unjustifiably narrowed the criminal provisions of HIPAA.

These targeted measures would bring credibility to the HIPAA enforcement system. There was good reason to go easy on covered entities, and help them come into compliance, when HIPAA first took effect. The HIPAA privacy rule was first announced in 1999, though, and it has been in full effect for over four years. Going forward, serious violations should lead to actual penalties. Only in this way will privacy and security practices improve. And only in this way will we have a credible case for the large expansion of electronic records that will come with the NHIN.

Some Steps May Be Appropriate to Adjust the Scope of Covered Entities

Staff has asked me for comments about the scope of who is considered a "covered entity" under HIPAA. HIPAA primarily applies today to health care providers, health insurers, and health clearinghouses. By contrast, HIPAA does not apply to many health websites or to services where the patients pay only by cash and credit card and there is no health insurance.[9]

The history of the HIPAA statute explains this odd state of affairs. As Congress in 1996 considered the large health legislation that ultimately was enacted as HIPAA, one important goal

[8] American Health Information Management Association, "The State of HIPAA Privacy and Security Compliance," (2006), *available at* http://www.ahima.org/emerging_issues/2006StateofHIPAACompliance.pdf.

[9] The Pew Foundation and Health Privacy Project address the scope of covered entities in their report "Exposed Online: Why the new federal health privacy regulation doesn't offer much protection to Internet users," (2001), *available at* http://www.pewinternet.org/pdfs/PIP_HPP_HealthPriv_report.pdf

was to simplify the health payments system and shift payments to electronic form. The "Administrative Simplification" part of HIPAA thus moved forward, and it applied precisely to those entities that were involved in the electronic payments system—providers, insurers, and clearinghouses (who convert records into standard electronic formats). Late in the legislative process, Congress realized that privacy and security protections should be included as part of the shift to electronic health payments. The scope of these privacy and security protections thus matched the scope of entities included in "Administrative Simplification."

Going forward, it is possible that additional entities should be covered by the HIPAA privacy and security rules. I recommend caution on this topic, however. To take one example, suppose that a person buys a book on breast cancer from an online book store. Should the entire book store be covered by HIPAA because some of the books are on medical topics?

The bookstore example reminds us that the most important regulatory decision is who will be covered by a rule. If Congress broadly increases the scope of "covered entities," then all of HIPAA's privacy and security requirements will apply to a potentially large number of organizations. Any expansion of that sort should be done only after careful study.

There is one area, however, where this committee may appropriately consider new measures. Important categories of government agencies are exempt from HIPAA but permitted by it to gain access to patient records. Under Section 512(b), public health agencies may receive records, and HIPAA does not apply to those agencies once they receive them. Of perhaps even greater concern, there are ways that law enforcement, homeland security, and national security agencies may be gaining access to large numbers of medical records. For instance, HIPAA's national security or public health exceptions might permit these agencies to receive health records to fight "bioterrorism." We know that the Total Information Awareness program led by Admiral Poindexter targeted such medical records. What we don't know is what sort of databases and data mining exist on Americans' health records in the name of national or homeland security. Jim Dempsey of the Center for Democracy and Technology is currently researching this topic. Attention to his forthcoming report and other oversight is warranted on how government agencies are using sensitive medical records.

Conclusion

This testimony has highlighted reasons to be cautious about preempting state privacy laws. It has suggested targeted measures to make HIPAA enforcement more credible, and has shown areas where oversight is appropriate on the definition of covered entity.

There are other important privacy and security issues that will arise in development of the NHIN. For instance:

- Authentication: how can we identify patients in the NHIN while avoiding creating one enormous database that becomes a risky source of failure?

- Consent: how can patients have an appropriately nuanced right to consent where in the NHIN their records will go, and for which records?

- Audit: as the NHIN links large numbers of organizations, how will audits and other controls enable the organizations to trust that appropriate safeguards are being implemented?

Discussion of each of these issues, and many others, is contained in Connecting for Health's Common Framework. I know of no better resource for understanding how to build privacy and security into the next generation of America's electronic health records.

My thanks to the committee for inviting me to participate today.

Mr. CLAY. Thank you, Mr. Swire.

Let me thank the entire panel for their testimony today.

We will begin the question period under the 5-minute rule, and I will begin with a general question for everyone to comment on. Many electronic health care tools such as electronic health records and internet-based personal health records are available to consumers today. The country, however, is still lacking an established nationwide approach for ensuring that personal health information will be protected from inappropriate disclosure. Do you believe that the implementation of health IT is beginning to out-pace the development of overall privacy policies and practices?

We will start with Ms. Grealy.

Ms. GREALY. Well, as I said, both from my experience as heading up the Healthcare Leadership Council and formerly with the American Hospital Association, as well as my personal experience dealing with health care for my family, providers took the HIPAA privacy rule very, very seriously. They put in place compliance plans, a lot of education, and this was throughout all of the covered entities, the various business associates. I am not sure we often recognize just how much went into making sure they understood the HIPAA privacy rules and they were in compliance.

The rules are very complex. I just want to touch on, I think, the approach that HHS and the Office of Civil Rights has taken is really the proper approach. They could have taken a "gotcha" approach, and, you know, every time we find you have made just the slightest error we are coming after you with civil and monetary penalties or criminal penalties. I think, instead, what they did was to develop a partnership. We want this rule to work, and so we have partnered with providers and others to educate them.

Of the 27,000 complaints that have been registered, I think if you delve into them, if you talk with the people at the Office of Civil Rights you will find that many, many, the vast majority, were really a misunderstanding of what was required by the privacy rule. In fact, many times we have run into what I would call hyper-compliance, where we have providers unwilling to share information with those who could benefit from it because they throw up HIPAA doesn't allow me to do that. So we really have to strike that appropriate balance.

As we move into the electronic world, security measures are in place. I think we also sometimes lose sight that these electronic medical records can be much more secure than the paper records that have been sitting in file cabinets and physicians' offices. Oftentimes you have no way of determining who has accessed those records, unlike in the electronic world where you can establish an audit trail. You can really determine who has accessed that and whether it is appropriate. You can password protect it.

So I think we have a framework. We may have to modify it. You can tell from the GAO testimony that there is a lot of work going on at HHS, at AHIC, the National Committee on Vital Health Statistics, to determine what is appropriate in this electronic world. But remember, this all started because people were concerned about the electronic transmission of personally identifiable health information. That is what started the HIPAA statute and resulted in the HIPAA privacy rule. So I don't think we need a wholesale

revision of it. We may need some tweaking of it. But I think right now it is workable, and a lot of providers are spending a lot of time and resources that don't go to direct patient care, but instead go toward compliance. I think we have to be very, very careful in terms of how we use those resources.

Mr. CLAY. Thank you, Ms. Grealy.

Mr. Pickard.

Mr. PICKARD. Yes. I would have to agree, and I think that it is not a question of the technology but more about the actual policies. I do believe that HIPAA has provided a good framework, and I think where we run into challenges or where we will run into challenges are the other entities, the other types of entities outside of the HIPAA boundaries, the covered entities that are now faced with handling health information. So I believe that is probably where we run into challenges associated with HIPAA. That, again, kind of brings us back to an important point or important principle within my testimony, and that is that the confidentiality and privacy protections follow the information, no matter where it goes or where it resides or how it is accessed or handled.

Mr. CLAY. How about you, Mr. Swire?

Mr. SWIRE. Thank you, sir.

A fairly simple point. HIPAA came about when we made a shift for payment records from paper to electronic, so you would file with Medicare, insurance companies electronically, and Congress said in 1996 let's do privacy and security with that.

We are now in chapter two, and chapter two is the shift for clinical records, your x-rays and all the rest of those things, and we are now building the systems for the first time to really move clinical records, so we should build those systems right for this generation like we tried to build systems right for the payments generation, and that is our job together.

The easiest time to get privacy and security right is when you build it the first time. It is much harder to patch later. That is where Congress can take a leadership role and make sure we do it.

Mr. CLAY. Thank you for that response.

Mr. Hodes.

Mr. HODES. Thank you, Mr. Chairman.

Professor Swire, I am interested in and appreciate your condensed version of arguments about preemption and what we might lose by it, because really I think that goes to the heart of policy issues that Congress is facing in dealing with the questions of a national health information network versus leaving it to what is clearly a rapidly evolving patchwork of regulation. You point out that we have HIPAA as, call it, a baseline, but that many States have—in fact, I think all the States have dealt with other medical information of a very sensitive kind that HIPAA simply doesn't deal with. So I take to heart your point about not rushing too quickly to simply say HIPAA is the standard and that is the national standard and that is where we are leaving it.

If we were to look at the national picture, which I am sure you have much more than I have, how would you balance, in looking what the various States have done in terms of the issues you have raised on pages three and four of your report—mental health

records, HIV, and all that—if Congress was inclined to try to set some national standard, mindful of your warnings? How would you suggest we go about looking at what the States have done? Should we simply say we are going to take the best standards from whichever State best protects privacy and security of people and that is the one we are going to use for HIV, and similarly we are going to look at mental health records and take the best one that we can get from State B, and then we are going to incorporate it with this other baseline and call it a Federal standard? What do you think?

Mr. SWIRE. Well, we could go on for quite some time——

Mr. HODES. I know.

Mr. SWIRE [continuing]. To try to figure out how to do that, but——

Mr. HODES. I have only got 5 minutes.

Mr. SWIRE. I know, and I will try to do it in about four sentences. Not really.

The first point is best does not mean stricter or less strict. You can't avoid making some judgments here, so when it comes to HIV data you have a public health issue if people won't get tested, and if you repeal for big cities' HIV protections you could face public health risks, and that doesn't seem like a good idea to me.

But I think one step here is I think that HHS and the Government can play a much better role in helping us all understand what the State laws are, and here is a specific thing. There is this RTI study—that is the contractor for HHS—and they have gone and done studies of, I think, 34 States. I have been told by somebody who has been near the process that they are not planning to release the surveys from the States to the public. It seems to me if Government is going to spend contractor money to try to figure out what all these State laws mean, they reduce compliance costs for everybody if we get that information out to everybody, so just a much better job of education and getting the information out there so that people don't have to go to expensive law firms to try to figure it out. That is one step toward knowing what needs to be done.

Ms. GREALY. Congressman, I would like to comment——

Mr. HODES. Please. Thank you.

Ms. GREALY [continuing]. Because we undertook one of those very expensive studies, $1 million investment, to have a tool where providers could check to see what is the State law, what is the variation. That still requires time. It is a lot of money to maintain that system, and I don't think it addresses your question. I don't think it really gives us a workable national standard. Just because we have the information from the RTI study, we still have all this variation.

We don't have to sacrifice privacy to develop this standard. Again I reference Section 6 in H.R. 4852, which really set out a process. Let's look at the States, let's study the variation, and then come up with recommendations as to what would be the appropriate rule in those very sensitive areas. We have done it for mental health to a certain degree in the HIPAA privacy rule, but we certainly could improve it in those other areas.

Mr. HODES. Thank you.

Mr. Pickard, did you want to comment?

Mr. PICKARD. No.

Mr. HODES. Thank you.

Mr. Chairman, I yield back. Thank you very much.

Mr. CLAY. Thank you for that line of questions.

I asked this question to GAO during the first panel and would like to hear your thoughts on the topic. A significant problem with HIPAA is that it does not cover all entities that possess or utilize personal health information. Some life insurers and research entities not involved with the treatment of patients fall outside the rules. In your work, have you analyzed this problem? And how significant is it, in your view?

Let's start with Mr. Swire.

Mr. SWIRE. OK. So this has to do with who should be covered entities, and the statute sets that forth. HHS doesn't have a lot of wiggle room on that, so it would have to come from Congress.

I think that for life insurance it is not such a big program. Graham-Leach-Bliley applies there. But in my testimony I point out that if you say anything that touches medical data, like I buy a breast cancer book for somebody on Amazon, we don't want to suddenly have HIPAA kick in just because they mention the word health, and so how to expand it is something that you have to be careful about.

One area of concern is that public health agencies are not subject to Federal laws, and law enforcement when it grabs health data, and there may be some work to be done on the Government's side to make sure that effective protections are in place, especially if they are trying to gather lots of bio-surveillance kinds of things going forward.

Mr. CLAY. Mr. Pickard.

Mr. PICKARD. Yes. If I could just say, that is an important question. I think that our association, AHIMA, strongly believes in harmonization of all of the privacy protections across all entities. When you look at the personal health records, when HIPAA was developed personal health records were barely being talked about. In a university setting with student records there is a lack of harmonization, as I mentioned in my testimony, between the FERPA, or Family Education Rights Privacy Act, and HIPAA. There are differences. And so I think it is an important question, and I think that, again, I agree it is one that will require answers and consideration as we move forward.

Mr. CLAY. Thank you.

Ms. Grealy, any thoughts?

Ms. GREALY. Well, as always, it is a balancing question. We want to make sure that we are not stifling innovation, as we have. I mean, I think we are finally beginning to see patients becoming more engaged in helping to manage their health care, and getting them engaged with personal health records I think is a very positive thing. We want to make sure that they feel very secure when they are sharing that information.

Now, is the best way to go about that, make everyone a covered entity? Is it better to make them business associates? I think we just have to make sure that the rules are clear, that we don't have conflicting standards out there. So if you start expanding business associates, making them covered entities, they may be in one sense

a business associate, have to comply with a covered entity's rules, but then in another setting they become a covered entity, and they all hold a different set of standards.

So, again, we know that there is work going on in this area. I know AHIC is looking at it. We are going to be testifying before them on Friday. But, again, just carefully looking at those and making sure that we are not getting into over-regulation and stifling the innovation that is really taking place out there.

I think one of the most important things I heard from the GAO panel, and something that we really have to focus on, is educating the public, communicating to them why do we want this information, but, more importantly, why is it good for you as a patient for us to have this information. Why do we want it? How are we going to share it? And how are we going to protect that information and keep it secure? So they know under HIPAA and various State statutes we can't disclose it to their employer, we can't disclose it to the newspaper, we can't disclose it to their neighbors. But we have to assure people that it is important for their health and for the health of future generations for us to have a workable privacy rule that allows for the necessary flow of health information.

Mr. CLAY. Along those same lines, there is significant debate concerning the most effective way to obtain patient authorization for the disclosure or sharing of personal health information. For a national health information network to be successful, doesn't it require a stronger uniform privacy standard that requires affirmative consent from a patient for all information disclosure? And yes, we can start with you. I would like to hear comments from the entire panel.

Ms. GREALY. I have the great benefit of every once in a while getting out there and talking to the real people that are actually doing this. I was just in Delaware, where they are doing a demonstration project with a health information network. We talked about this. Let's call it opt-in versus opt-out.

I am going around and asking this question: how would your data exchange system work if it had to be an opt-in? If you are the Mayo that has a century worth of data, longitudinal studies, how would it work if you had to have an opt-in as opposed to you have the information, you give people the opportunity to opt-out of it? But if you had to go to each individual patient, to each individual subject that you want included, and get their affirmative decision to be included and to share their electronic medical record, I think it would halt the system.

If we have to make a decision between the two, certainly opt-out is going to be better.

Mr. CLAY. Mr. Pickard, any comments?

Mr. PICKARD. Yes. Again, I think this is probably an area where AHIC is, in terms of their Privacy and Security Committee is looking into these types of issues.

I can tell you in the State of Tennessee, with our health information exchange we have run up against this very question or this very issue, and we have put in protocols to enable patients to opt in or opt out, and then certainly you have the whole concept of patient identification. But, again, I think it is an important issue.

Mr. CLAY. Mr. Swire.

Mr. SWIRE. Thank you. So the one way this comes up is if somebody sees a psychiatrist or gets substance abuse or something else and they say, look, I don't want this going out to everybody everywhere. So one idea of consent or authorization is some way for the patient to say, hold on, not this.

I think it makes sense to a lot of people that some sort of permission for patients or some sort of control over that might make sense.

Now, we can talk opt-in/opt-out. Some of the systems don't want to have an opt at all. They just want to say we are going to sign everybody up. I think that is a concern. So if you don't want to be in at all, if you don't want to just sort of have my doctor puts everything in and I have no control over that, I don't think that is the right place to be. The question is what point, for how many choices, will a patient have any say.

I worked on Markle's Connecting for Health Task Force, and they have a write-up on this that I think goes through it in a sensible way, and I think you end up with an opt out where that is realistic where patients say, look, it generally goes in, but if I say it doesn't we should try to build it so it doesn't go in.

Mr. CLAY. Just to pause after hearing the three different responses, what is the damage? What is the harm if someone other than a health care provider gets a copy of an x-ray or they get a record of a prescription? What do you think the harm is?

Ms. GREALY. I think the concern is that the health care provider might not get the x-ray. I mean, I am not even talking about disclosures to those that really shouldn't have the information. We are talking about patients saying, no, provider, the physician treating me cannot have this information. So we have to be very, very cautious, again, in that balance of making sure, and there may be a system of, you know, flagging it so the physician knows I don't have all the information, I had better check with this patient.

I am not sure how that translates when we are trying to build data bases to improve the quality of health care, to improve treatment for disease, if we have a lot of critical missing information.

Mr. CLAY. Well, like the example you use in your testimony, the pharmacist should have relayed to both physicians for your father what medicines?

Ms. GREALY. If this were something that he was getting at a pharmacy, you are right. CVS, one of our members, they have gone electronic, so they can do those alerts. But these were services, these were hormone shots, one being given in the oncologist's office and the other being part of the dialysis center treatment. There is no pharmacist in the picture, no electronic medical record to exchange that information, and so no way to alert.

Mr. CLAY. Mr. Pickard, any thoughts?

Mr. PICKARD. Again, I think—and I said this in my testimony—I think we need to move away from thinking about the type of information and the entity and make sure that the privacy protections do follow the health information wherever it resides.

Let me just share. If I am an employee, I want the capability to opt out and to perhaps not have my employer have certain types of information. This is particularly important in today's environment where a lot of employers or insurances, for that matter, are

developing personal health record tools for employees or subscribers. I think as an employee or an insurance subscriber, I should have that right to opt out of that.

Mr. SWIRE. Just one point to add on is that some of the most sensitive kinds of data that I have been talking about, the mental health and substance abuse, genetic, or whatever, are only protected by State law, so even if x-rays aren't, these other things are only protected by State law, and if we were to harmonize at the national baseline then those psychiatric notes, the substance abuse things, and the rest could be going through the system, and that is a reason not to preempt too strictly or not to preempt at a low level.

Mr. CLAY. Let me ask this. This is a question for the entire panel. There have been long-term concerns on how health information is treated differently under institutions that are also covered under different privacy regulations, such as Family Educational Rights and Privacy Act of 1974. Under the privacy rule, records protected by FERPA are not covered by the privacy rule; therefore, even if the information contained in an education record is health related, the privacy rule does not apply.

Is this an area where conflicts ought to be addressed in order to harmonize the way in which patient information is protected?

Ms. Grealy, we will ask you first.

Ms. GREALY. Well, I think one of the things that those that actually have to do compliance are always looking for is; give me uniformity. Make it simple. Don't have one set of standards here, another set of standards there. So I think any way we can harmonize these requirements is a positive thing.

Mr. CLAY. Mr. Pickard.

Mr. PICKARD. I agree. And let me just share, working in a university, you know, we interact and deal with both HIPAA regulations as well as FERPA regulations, and if I am a student and let's say if I have a medical condition that requires me to live off campus, I have to submit what actually becomes part of my academic record health information, and there is a lack of standardization in terms of how that information may or may not be handled. So I agree. I think there needs to be a harmonization across all of these different laws.

Mr. CLAY. Thank you.

Mr. Swire.

Mr. SWIRE. I am going to disagree on the FERPA one. I will just explain why. That was an issue that I worked on extensively during the rule and the comments from the schools, associations, and the rest. The logic at the time—and maybe it is different today—was with school nurses in high schools all over the country, rural grade schools, all the rest, if we harmonized to HIPAA, which is what AHIMA recommends and is worth considering, if we harmonize to HIPAA then the school nurse in that grade school out in a rural area would have to do full HIPAA compliance. And it wasn't clear that was the big risk, and it was clear that there would be a whole compliance thing to do if that happened.

So the idea there was we thought that there was a pretty reasonable FERPA regime in place, that the school nurses shouldn't suddenly have to do more, and that was a sensible way to go.

Now, it does mean that universities like Vanderbilt get a double whammy, because they get students and then they get some other folks who are HIPAA, and suddenly they get both. In some ways maybe Vanderbilt people are so smart they can handle it, but maybe not every school nurse has to do HIPAA.

So I am not really sure how you harmonize, because if you harmonize that everybody is HIPAA, then it is the school nurses of America that will be here next time.

Mr. CLAY. Speaking of universities, Mr. Swire, I will ask you and then go down the line. Mr. Mark Rothstein of the University of Louisville has written extensively on the use of compelled authorizations for personal health information by employers for job applicants, life insurers for those applying for coverage, and other noncovered entities. If the current privacy rule does not regulate PHI once it is released to a third-party entity not covered under the rule, shouldn't we re-examine who will be covered when receiving electronic health information?

Mr. SWIRE. That is a great question, and it wouldn't be easy to legislate, but here are a couple of points that come up.

So right now you can't have compelled authorizations for health care providers. If you show up at the ER and you are rolling in on the gurney, they can't say, sign here or we won't treat you, and you sign away everything. That is in HIPAA.

The thing was, when HIPAA rules were written, HHS could do that—that is covered entities—but HHS had no jurisdiction over the employers of America. That just wasn't in the statute, so there was no choice in writing the rule about what to do for employers. That is a choice that only Congress can decide to step into.

If you want to say, as Congress, we are going to treat the employers the way we treat the hospitals, you can't require these authorizations as a condition of being employed here, that is a decision Congress can make. You are going to hear it from the employers. And sometimes employers will say we need this to figure out if they can lift the heavy loads or we need it for some other job-related thing. But that is what you would have to work through, and it would have to be statute. It can't be by reg.

Mr. CLAY. Thank you.

Any comments on that, Mr. Pickard?

Mr. PICKARD. Yes. We are seeing many, many different types of entities outside of the HIPAA-covered entities and business associates that are handling health information. Again, this goes back to our principles I shared earlier, and that is that we really look to confidentiality protections following the health information, no matter where it resides, and there needs to be a national floor for handling health information.

Mr. CLAY. OK. Ms. Grealy.

Ms. GREALY. I talked with a few of, I think, entities that people are referring to. Revolution Health Care is one that is really getting into working with consumers, developing a personal health record that they can access through the internet. They have a contractual relationship with the consumers that they are dealing with, and they say that they are HIPAA compliant, even though they are not a covered entity; that they feel it is a good business practice. They want the trust of the consumers that they are deal-

ing with, and it is in their best interest to make sure that they have a high level of security and protecting that information.

So I think all of us have mentioned we know that AHIC, HHS, and others are really exploring these issues, and I think that is really the appropriate place; that we need to look at it carefully; make sure, as I said earlier, that we are not stifling innovation by expanding the reach of a heavy regulatory scheme; and make sure that it is balanced well, because I don't think we want to snuff out the innovation that is going on out there, but we do want to make sure that this information is protected.

Mr. CLAY. All right. Thank you.

Let me thank the entire panel for their testimony and their answers. We have certainly covered some ground today. This is a very complex issue. As the Congress takes this issue on of health information technology and how we actually protect the privacy of citizens throughout this country, patients, we will certainly rely on your expertise, and this hearing has been helpful in shedding light on this. Let me again thank you all for your testimony today.

That concludes this hearing.

[Whereupon, at 3:30 p.m., the subcommittee was adjourned.]

[Additional information submitted for the hearing record follows:]

Testimony Before the
Subcommittee on Information Policy, Census and National Archives

Protecting Patient Privacy in Healthcare Information Systems

Statement of

Robert Kolodner, M.D.

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

June 19, 2007

Honorable Chairman Clay, thank you for the opportunity to submit testimony on behalf of the Department of Health and Human Services (HHS) about protecting patient privacy in healthcare information systems.

Introduction

On April 27, 2004, the President signed Executive Order 13335 announcing his commitment to the promotion of health information technology (health IT) to improve efficiency, reduce medical errors, improve quality of care, and provide better information for patients and physicians. 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 IT, 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 the 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."

Safeguarding personal health information is essential to our national strategy for health IT. A strategy devoid of measures to ensure privacy and security would neither advance our interests nor those of the American people. 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

The movement towards interoperable electronic health records will create both new challenges and new opportunities with respect to protecting the privacy and security of health information. 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.

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 Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, the HIPAA Security Rule, and the 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 exchanged by HIPAA covered entities in the health IT environment while allowing best practices to emerge. However, there are differences between Federal laws, State laws and business practices, which can provide additional challenges for the sharing of health information in a private and secure manner, an issue that is currently being examined.

The number, type, and sophistication of tools that 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.

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 while information remains private and secure.

Ensuring Privacy and Security Protections through Health IT

Protecting health information in an interoperable electronic environment requires a coordinated effort by all stakeholders. At HHS, we've leveraged existing foundations; created new public-private collaborations; and partnered with other federal departments, states, health care organizations, and consumers to continue this critical dialogue. Privacy and security policies must be coordinated and developed openly – with abundant public input – in order to ensure a high degree of trust. Many privacy and security frameworks are in existence, and we need to leverage the work that has been done as we apply these principles in the area of health IT. Further, this is both iterative and informed. Technological solutions are being advanced to

support the confidentially of patient data and to accommodate current and future policy decisions.

To that end, HHS has initiated several projects focusing on the development and harmonization of privacy and security standards. HHS directed the establishment of the Healthcare Information Technology Standards Panel (HITSP), which has focused on the harmonization of standards, including those related to privacy and security. ONC continues to work closely with the Certification Commission for Healthcare Information Technology (CCHIT) to develop certification criteria for electronic health records and networks. The Department has also been actively advancing the Nationwide Health Information Network (NHIN) Initiative, which will ensure consumers have an active role in determining the uses of their health information while supporting local and state policies.

We are working to achieve a balance between our technical capabilities to exchange health information and the privacy and security policies that protect it. Appropriate privacy and security policies must account for available technologies and anticipate technological improvements, without being outpaced by innovations developed for the NHIN and interoperable health IT. At the June 12, 2007, American Health Information Community meeting, I described the process HHS is undertaking to develop a privacy and security framework that will meet the expectations of health care consumers and foster the adoption of practices that promote trust in this new environment. One of our first steps will be to engage public and private entities, including the general public, to refine and build consensus around a set of privacy and security principles to protect individuals' health information in an interoperable electronic environment applicable to both the public and private sectors.

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.

Privacy and Security Solutions for Interoperable Health Information Exchange
The Privacy and Security Solutions contract awarded to RTI International (RTI), co-managed by the Office of the National Coordinator for Health Information Technology (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 and one nationwide meeting in March 2007, where they exchanged experiences with regional counterparts and discussed the appearance of common themes such as differing applications and interpretations of HIPAA regulations, state consent laws, and state variations in protections provided to sensitive information, such as HIV/AIDS information and mental health records. This summer, RTI will publish three reports that describe the variations in organization-level business policies and state laws which pose challenges to private and secure electronic health information exchange; state plans to implement solutions to address those challenges; and recommendations for the federal government to consider. Starting in July, the states and territories that are part of the HISPC will begin operationalizing their implementation plans as well as preparing collaboration strategies with all states and territories for regional and multi-state solution development.

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, is 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, one of three taskforces under the State Alliance, is responsible for examining privacy and security issues. With coordinated input from HISPC participants and testimony from experts in health privacy and security, this taskforce will recommend to the State Alliance policies for states and territories to adopt (and vehicles to facilitate adoption) that will encourage, where appropriate and without diminishing protections, uniformity in their health IT privacy and security practices.

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 with best practices 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. On the basis of a recommendation issued jointly by three of its workgroups (Chronic Care, Electronic Health Records, Consumer Empowerment), the AHIC created a workgroup in the summer of 2006 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 workgroups and their breakthrough projects. The members for this Confidentiality, Privacy, and Security workgroup 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 to the AHIC on patient identity proofing were advanced and accepted after deliberation by the AHIC on January 23, 2007, for recommendation to HHS. In the next phase of the NHIN Initiative, selected contractors will be required to meet privacy and security functional requirements and specifications derived from NCVHS and relevant AHIC recommendations (including the CPS recommendation above) as well as other health IT initiatives. Additionally, on June 12, 2007, the AHIC accepted a recommendation from the workgroup that expressed how and to whom privacy and security protections should apply in an electronic health information exchange environment. Its letter to the AHIC (available at http://www.hhs.gov/healthit/community/meetings/m20070612.html) describes in greater detail the work undertaken thus far and the workgroup's next steps.

In addition, the ONC is currently working to ensure that the AHIC CPS workgroup works collaboratively with the National Committee for Vital and Health Statistics, to address the challenges posed by secondary uses of health information in an electronic environment including those related to non-HIPAA covered entities.

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. 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.

CCHIT has set criteria for the certification of ambulatory EHR systems, including twenty-nine security criteria that EHRs had to meet to achieve certification in 2006. As of May 2007, CCHIT has certified over 80 ambulatory EHRs that meet these security criteria and several additional criterion for functionality and interoperability. As new privacy and security standards are harmonized, they will be incorporated into future versions of the certification criteria.

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.

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 overlaps and gaps in standards where they are inadequate or unavailable and specifies the use of those standards to advance interoperability.

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. Recently, HITSP formalized the workgroup it created to focus on privacy and security by establishing a technical committee to identify, evaluate, and select standards for privacy and security to support the current suite of Interoperability Specifications and 2007 use cases.

Nationwide Health Information Network (NHIN)
In November 2005, ONC awarded contracts to four consortia to develop prototypes capable of demonstrating potential solutions for nationwide health information exchange. This initiative is foundational to the President's vision for the widespread adoption of secure, interoperable health records within 10 years. The NHIN's vision is to become a "network of networks" where state and regional health information exchanges and other networks that provide health information services work together, through common architecture (services, standards and requirements), processes, and polices to securely exchange information. In particular the NHIN will: provide consumers with capabilities to help manage the flow of their information; allow health information to follow the consumer; provide critical information to clinicians at the point of care; and improve healthcare, population health, and prevention of illness and disease.

The first year of the NHIN initiative produced four prototype architectures and a number of architectural products that will be used in the second year of this initiative. A critical portion of the required NHIN prototype deliverables was the development of security models that directly address systems architecture needs for securing and maintaining the confidentiality 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 was 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 delivered 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.

This second year of the NHIN initiative will involve the demonstration of trial implementations in real-world healthcare environments while maximizing the use of existing infrastructure. The trial implementations will be functional across healthcare markets in the service area selected as well as with other participants in the NHIN cooperative and specialty networks involved in use case activities. Moreover, trial implementation sites will be required to demonstrate "core" services, including a suite of consumer services. These services will, in a demonstrable way, empower consumers with knowledge and choice. For certain interactions within a trial implementation, consumers will be given an increased role in determining the confidentiality, privacy, and security of their health information.

Conclusion

Health IT privacy and security policies and their associated technological solutions cannot be developed in a vacuum. A key component for assuring 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 together closely 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.

Protecting health information is of the utmost importance and essential to the success of interoperable electronic health information exchange. Proper policies that instill confidence and trust must evolve with technology advancements and vice versa. Not letting one get too far ahead of the other is a concern we share and are working hard to continue to manage. As a leader in this area HHS has invested in multiple coordinated initiatives to ensure health information will be protected as we enter this new era of health and care.

Mr. Chairman, thank you for the opportunity to submit testimony today.