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

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

Statement of

Robert Kolodner, M.D.

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

February 1, 2007

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

Introduction

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

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

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

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

Health Information Privacy and Security

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

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

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

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

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

Ensuring Privacy and Security Protections through Health IT

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

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

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

The 34 states and territories that are part of the Health Information Security and Privacy Collaboration (HISPC) under the Privacy and Security Solutions contract participated in ten regional meetings in the fall of 2006 where they exchanged thoughts with regional counterparts and discussed the appearance of common themes such as misinterpretations of HIPAA, state consent laws, and the protection variations states provided to specific disease information, such as HIV/AIDS. In November 2006, the HISPC states and territories submitted their interim assessment of variation reports to RTI and will complete the remainder of their work this spring, including several other interim and final reports. In April 2007, the states and territories will advance implementation plans that will not only inform health information exchange initiatives in the states and territories that created them, but will serve as input to other ONC-coordinated efforts such as the State Alliance for E-Health's Health Information Protection taskforce.

State Alliance for E-Health

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

Development of Best Practices for State HIE Initiatives

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

American Health Information Community: Confidentiality, Privacy, and Security (CPS) Workgroup

In September 2005, the Secretary established the American Health Information Community (AHIC), a federally-chartered advisory committee made up of key leaders from the public and private sectors, charged with making recommendations to HHS on key health IT strategies. In the summer of 2006, the AHIC on the basis of a recommendation issued jointly by three of its workgroups (Chronic Care, Electronic Health Records, Consumer Empowerment) created a workgroup specifically focused on nationwide privacy and security issues raised by health IT activities and the findings of the other AHIC workgroups – privacy and security are one of the most consistent threads between each of the groups and their breakthrough projects. The workgroup members were carefully selected to assure that there was sufficient privacy and security expertise, sufficient consumer input, and representation of relevant health care stakeholders that may be affected by any recommendations developed. The workgroup's first set of recommendations on patient identity proofing were advanced and accepted after deliberation by the AHIC on January 23, 2007, for recommendation to the Secretary of HHS. These recommendations, if adopted by HHS and others, together with existing protections, will inform the AHIC's breakthrough activities and serve as a model for the private sector in this area. The workgroup is currently prioritizing its next issue and is contemplating a privacy focused discussion in collaboration with the Consumer Empowerment workgroup on the personal health record (PHR) environment and associated privacy protections.

American Health Information Community: Personalized Healthcare Workgroup

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

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

The Certification Commission for Healthcare Information Technology (CCHIT)

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

Through January 2007, CCHIT has certified 55 ambulatory EHRs that meet these security criteria among others for functionality and interoperability. In 2007 and 2008, the CCHIT will develop security criteria to certify inpatient EHR systems and network services. In addition, CCHIT updates previously published certification criteria on an annual basis, and as a result, additional security criteria for ambulatory EHRs were added for the 2007 round of testing. The certification process CCHIT has developed promotes well-established, tested, security capabilities in health IT systems and helps make certification a major contributor to protecting the privacy and confidentially of the data these systems manage.

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

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

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

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

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

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

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

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

Conclusion

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

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

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

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