United States Government Accountability Office

GAO

Testimony

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

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

HEALTH INFORMATION TECHNOLOGY

Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy

Statement of
Linda D. Koontz
Director, Information Management Issues

David A. Powner
Director, Information Technology Management Issues

Abbreviations

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

February 2007

HEALTH INFORMATION TECHNOLOGY

Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy

GAO Accountability · Integrity · Reliability

Highlights

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

Why GAO Did This Study

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

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

What GAO Recommends

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

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

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

What GAO Found

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

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

Challenges to Exchanging Electronic Health Information

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

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

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

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

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

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

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

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

was performed in accordance with generally accepted government auditing standards.

Results in Brief

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

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

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

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

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

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

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

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

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

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

Background

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

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

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

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

[5]Executive Order 13335.

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

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

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

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

Health Insurance Portability and Accountability Act of 1996

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

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

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

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

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

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

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

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

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

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

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

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

Source: GAO analysis of HIPAA Privacy Rule.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The Health Care Industry Faces Challenges in Protecting Electronic Health Information

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

Table 2: Challenges to Exchanging Electronic Health Information

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

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

Understanding and Resolving Legal and Policy Issues

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

Ensuring Appropriate Disclosure

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

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

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

Implementing Adequate Security Measures for Protecting Health Information

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

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

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

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

1. Identify milestones and the entity responsible for integrating the outcomes of its privacy-related initiatives, including the results of its four health IT contracts and recommendations from the NCVHS and AHIC advisory committees.

2. Ensure that key privacy principles in HIPAA are fully addressed.

3. Address key challenges associated with legal and policy issues, disclosure of personal health information, individuals' rights to request access and amendments to health information, and security measures for protecting health information within a nationwide exchange of health information.

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

[14]GAO-07-238.

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

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

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

Summary

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

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

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

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

Contacts and Acknowledgments

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

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