United States Government Accountability Office

GAO

Report to Congressional Requesters

January 2007

HEALTH INFORMATION TECHNOLOGY

Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy

GAO-07-238

January 2007

HEALTH INFORMATION TECHNOLOGY

Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy

GAO Accountability · Integrity · Reliability

Highlights

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

Why GAO Did This Study

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

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

What GAO Recommends

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

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

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

What GAO Found

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

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

Challenges to Exchanging Electronic Health Information

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

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

Contents

Abbreviations

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

GAO
Accountability * Integrity * Reliability

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

January 10, 2007

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

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

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

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

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

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

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

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

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

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

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

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

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

Results in Brief

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Background

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

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

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

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

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

Federal Government's Role in Health Care

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

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

[8]Executive Order 13335.

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

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

Need for a National Strategy and Adoption of Interoperable Health IT

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

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

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

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

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

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

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

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

Legal Privacy Protections for Personal Health Information

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

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

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

Early Federal Laws Enacted to Protect the Privacy of Health Information

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

Health Insurance Portability and Accountability Act of 1996

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Source: GAO analysis of HIPAA Privacy Rule.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(Continued From Previous Page)

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

Source: GAO analysis of HHS data.

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

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

The Health Care Industry Faces Challenges in Protecting Electronic Health Information

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

Table 3: Challenges to Exchanging Electronic Health Information

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

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

Understanding and Resolving Varying Legal and Policy Issues

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

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

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

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

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

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

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

Ensuring Appropriate Disclosure

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

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

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

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

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

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

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

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

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

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

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

Implementing Adequate Security Measures for Protecting Health Information

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

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

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

Conclusions

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

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

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

Recommendation for Executive Action

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

Agency Comments and Our Evaluation

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

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

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

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

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

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

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

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

Linda D. Koontz
Director, Information Management Issues

David A. Powner
Director, Information Technology Management Issues

Objectives, Scope, and Methodology

The objectives of our review were to

- describe the steps the Department of Health and Human Services (HHS) is taking to ensure privacy protection as part of the national health information technology (IT) strategy and

- identify challenges associated with meeting requirements for protecting personal health information within a nationwide health information network.

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

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

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

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

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

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

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

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

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

Major Federal Health Care Programs

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

Table 4: Federal Programs

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

Source: HHS, VA, DOD, and OPM budget documents.

HHS Health IT Contracts

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

Table 5: HHS Health IT Contracts

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

(Continued From Previous Page)

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

(Continued From Previous Page)

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

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

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

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

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

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

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

(Continued From Previous Page)

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

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

[a]Strategy has been initiated.

[b]Strategy is under active consideration.

[c]Strategy requires future discussion.

Descriptions of Federal Laws for Protecting Personal Health Information

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

Table 7: Selected Federal Laws that Protect Personal Health Information

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

(Continued From Previous Page)

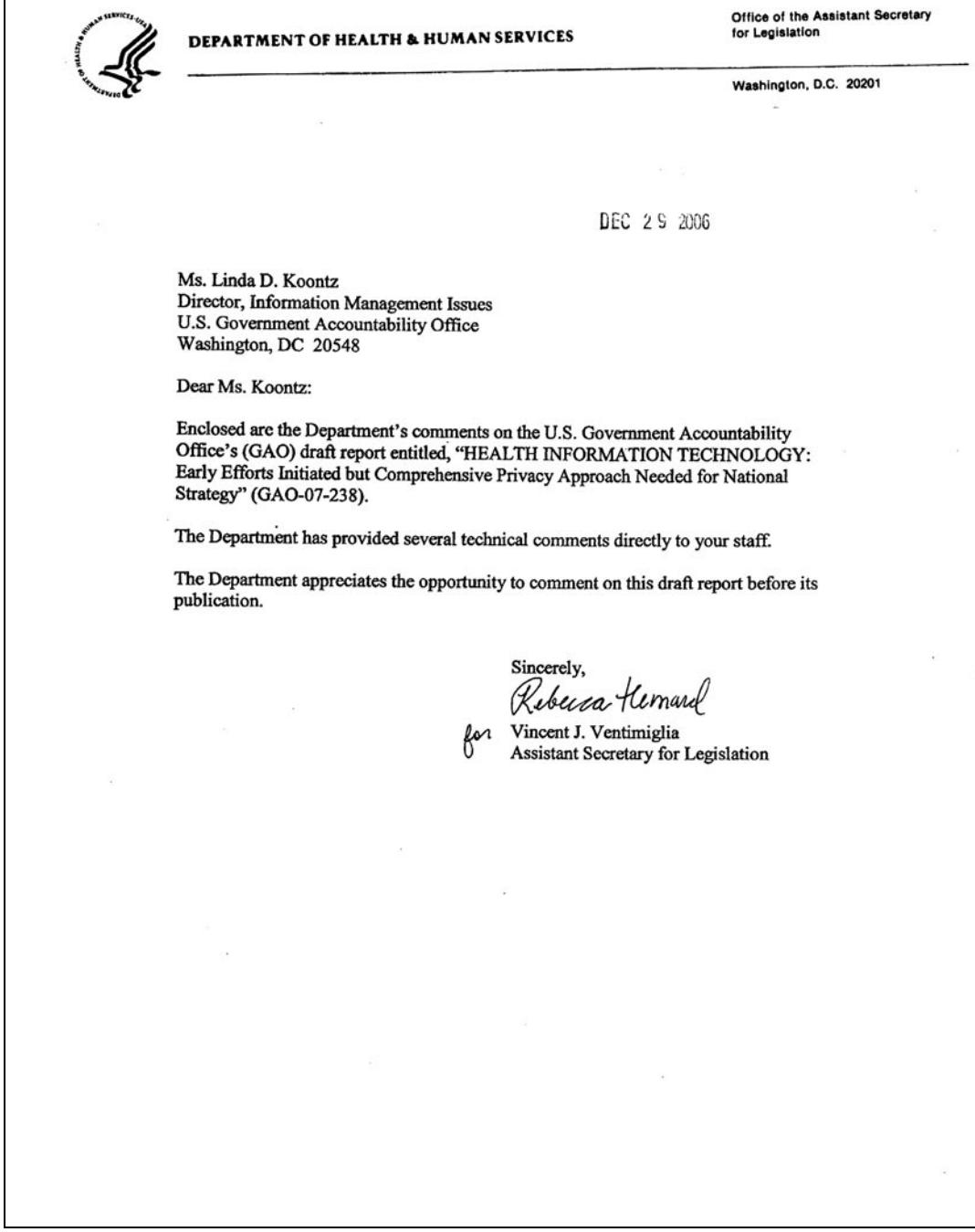
Law	
Social Security Act	Protected information: Individually identifiable records and information held by an agency regarding program beneficiaries' records and information that is transmitted to, or obtained by or from HHS, Social Security Administration (SSA), and their contractors incident to carrying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

(Continued From Previous Page)

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

Source: GAO analysis of federal privacy laws

Comments from the Department of Health and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Assistant Secretary for Legislation

Washington, D.C. 20201

DEC 29 2006

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

Dear Ms. Koontz:

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

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

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

Sincerely,

Rebecca Hemard

for Vincent J. Ventimiglia
Assistant Secretary for Legislation

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

General Comments

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

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

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

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

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

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

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

Existing Foundations

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

State and Organizational Efforts

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

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

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

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

Federal Activities

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

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

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

5

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

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

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

SUMMARY

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

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

7

Comments from the Department of Veterans Affairs

THE SECRETARY OF VETERANS AFFAIRS
WASHINGTON

December 27, 2006

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

Dear Ms. Koontz and Mr. Powner:

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

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

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

Sincerely yours,

R. James Nicholson

Enclosure

GAO Contacts and Acknowledgments

GAO Contacts

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

Acknowledgments

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

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