United States Government Accountability Office

GAO

Report to the 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

September 2008

HEALTH INFORMATION TECHNOLOGY

HHS Has Taken Important Steps to Address Privacy Principles and Challenges, Although More Work Remains

GAO-08-1138

September 2008

HEALTH INFORMATION TECHNOLOGY

HHS Has Taken Important Steps to Address Privacy Principles and Challenges, Although More Work Remains

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-1138, a report to the 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

Why GAO Did This Study

Although advances in information technology (IT) can improve the quality and other aspects of health care, the electronic storage and exchange of personal health information introduces risks to the privacy of that information. In January 2007, GAO reported on the status of efforts by the Department of Health and Human Services (HHS) to ensure the privacy of personal health information exchanged within a nationwide health information network. GAO recommended that HHS define and implement an overall privacy approach for protecting that information. For this report, GAO was asked to provide an update on HHS's efforts to address the January 2007 recommendation. To do so, GAO analyzed relevant HHS documents that described the department's privacy-related health IT activities.

What GAO Recommends

GAO recommends that HHS include in its overall privacy approach a process for ensuring that key privacy principles and challenges are completely and adequately addressed. In written comments on a draft of this report, HHS generally agreed with the information discussed in the report.

To view the full product, including the scope and methodology, click on GAO-08-1138. For more information, contact Valerie C. Melvin, (202) 512-6304 or melvinv@gao.gov.

What GAO Found

Since GAO's January 2007 report on protecting the privacy of electronic personal health information, the department has taken steps to address the recommendation that it develop an overall privacy approach that included (1) identifying milestones and assigning responsibility for integrating the outcomes of its privacy-related initiatives, (2) ensuring that key privacy principles are fully addressed, and (3) addressing key challenges associated with the nationwide exchange of health information. In this regard, the department has fulfilled the first part of GAO's recommendation, and it has taken important steps in addressing the two other parts. The HHS Office of the National Coordinator for Health IT has continued to develop and implement health IT initiatives related to nationwide health information exchange. These initiatives include activities that are intended to address key privacy principles and challenges. For example:

- The Healthcare Information Technology Standards Panel defined standards for implementing security features in systems that process personal health information.
- The Certification Commission for Healthcare Information Technology defined certification criteria that include privacy protections for both outpatient and inpatient electronic health records.
- Initiatives aimed at the state level have convened stakeholders to identify and propose solutions for addressing challenges faced by health information exchange organizations in protecting the privacy of electronic health information.

In addition, the office has identified milestones and the entity responsible for integrating the outcomes of its privacy-related initiatives, as recommended. Further, the Secretary released a federal health IT strategic plan in June 2008 that includes privacy and security objectives along with strategies and target dates for achieving them.

Nevertheless, while these steps contribute to an overall privacy approach, they have fallen short of fully implementing GAO's recommendation. In particular, HHS's privacy approach does not include a defined process for assessing and prioritizing the many privacy-related initiatives to ensure that key privacy principles and challenges will be fully and adequately addressed. As a result, stakeholders may lack the overall policies and guidance needed to assist them in their efforts to ensure that privacy protection measures are consistently built into health IT programs and applications. Moreover, the department may miss an opportunity to establish the high degree of public confidence and trust needed to help ensure the success of a nationwide health information network.

Contents

Tables

Abbreviations

HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
IT	information technology

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 17, 2008

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
United States Senate

Dear Mr. Chairman:

Advances in health information technology (IT) have the potential to improve the quality of health care, to increase the availability of health information for treatment, and to implement safeguards that cannot be applied easily or cost-effectively to paper-based health records. However, the automation of health information also introduces new risks to the privacy of that information. A September 2007 survey sponsored by the Institute of Medicine indicated that nearly 60 percent of the respondents did not believe that the privacy of personal medical records and health information was adequately protected by federal and state laws and organization practices.[1] According to the National Research Council,[2] medical information is often the most privacy-sensitive information that patients provide to others about themselves, and protecting medical privacy has long been recognized as an essential element in a health care system. Further, industry groups and professional associations have called for stronger privacy protection of personal health information.

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

[1]Institute of Medicine, *How the Public Views Privacy and Health Research* (Washington, D.C.: November 2007).

[2]The National Research Council is sponsored by the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The mission of the council is to improve government decision making and public policy, increase public education and understanding, and promote the acquisition and dissemination of knowledge in matters involving science, engineering, technology, and health.

and private sectors.[3] The order required the plan 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. In 2004, the Secretary of Health and Human Services, through the Office of the National Coordinator for Health Information Technology, documented a framework for health IT as the first step toward the development of a national strategy.[4] This framework stated that strengthening privacy protections for electronic personal health information was a critical health care need.

In January 2007, we reported on activities of the Department of Health and Human Services (HHS) and its Office of the National Coordinator for Health IT to identify solutions for protecting personal health information.[5] We noted that HHS was in the early stages of these activities and had not yet defined an overall approach for addressing key privacy principles and challenges, nor had it defined milestones or identified a responsible entity for integrating the results of these activities. Consequently, we recommended that the Secretary of Health and Human Services define and implement an overall approach for protecting health information that would (1) identify milestones and the entity responsible for integrating the outcomes of its privacy-related initiatives, (2) ensure that key privacy principles in the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[6] are fully addressed, and (3) address key challenges associated with the nationwide exchange of health information. Subsequently, the department's National Coordinator for Health IT agreed with the need for an overall approach to protect health information and

[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).

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

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

[6]The act provided for the Secretary of HHS to establish the first broadly applicable federal privacy and security protections designed to protect individually identifiable health information. Pub. L. No. 104-191 (Aug. 21, 1996), sec. 262(a); 42 U.S.C. 1320d-2. Throughout this report, when we refer to key privacy principles in HIPAA, we are referring to the privacy principles promulgated under HIPAA's Administrative Simplification provisions.

stated that the department was initiating steps to address our recommendation.

As you requested, we conducted a follow-up study of the Office of the National Coordinator's efforts to ensure the privacy of electronic personal health information exchanged within a nationwide health information network. Our objective was to provide an update on the department's efforts to define and implement an overall privacy approach, as we recommended.

To address our objective, we analyzed reports and other documentation of the Office of the National Coordinator's current health IT initiatives related to privacy. We also obtained and analyzed the department's documents describing plans and outcomes from the Office of the National Coordinator's health IT initiatives related to privacy, and we supplemented our analysis with interviews of officials from the National Coordinator's office to discuss the department's current approaches and future plans for developing and implementing an overall approach for addressing privacy protection within a nationwide health information network.

We conducted this performance audit from April 2008 through September 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Our objective, scope, and methodology are described in appendix I.

Results in Brief

Since we reported in January 2007 on HHS's efforts to protect electronic personal health information, the department has undertaken various initiatives that are contributing to its efforts to develop and implement an overall privacy approach. We recommended that this approach include (1) identifying milestones and the entity responsible for integrating the outcomes of its privacy-related initiatives, (2) ensuring that key privacy principles in HIPAA are fully addressed, and (3) addressing key challenges associated with the nationwide exchange of health information. In this regard, the department has fulfilled the first part of our recommendation, and it has taken important steps in addressing the two other parts. The Office of the National Coordinator for Health IT has continued to develop and implement initiatives related to a nationwide health information network, and these initiatives include activities that are

intended to address certain key privacy principles and challenges. For example:

- The Healthcare Information Technology Standards Panel defined standards for implementing security features in health IT systems that process personal health information.

- The Certification Commission for Healthcare Information Technology defined certification criteria that include privacy protections for both outpatient and inpatient electronic health records.

- State-level initiatives (such as the Health Information Security and Privacy Collaboration and the State Alliance for e-Health) have convened stakeholders to identify and propose solutions for addressing challenges to protecting the privacy of electronic health information faced by health information exchange organizations.

In addition, the Office of the National Coordinator has identified milestones and the entity responsible for integrating the outcomes of its privacy-related initiatives, as we recommended. Further, the Secretary released a federal health IT strategic plan in June 2008 that includes privacy and security objectives along with strategies and target dates for achieving them. The strategic plan also outlines the Office of the National Coordinator's plans for developing a confidentiality, privacy, and security framework to incorporate the outcomes of privacy-related initiatives, which it expects to publish by December 2008.

Nevertheless, while the aforementioned initiatives are significant to addressing privacy issues and challenges, they fall short of fully implementing our recommendation. Specifically, HHS has not defined, as part of its approach, a process for ensuring that all privacy principles and challenges will be fully and adequately addressed. Given the large number and variety of activities being undertaken and the many federal, state, and private-sector entities contributing to the health IT initiatives, it is important that the department and its Office of the National Coordinator define a process for ensuring that all stakeholders' contributions will be appropriately considered and that inputs to the privacy framework will be effectively assessed and prioritized to achieve comprehensive coverage of all privacy principles and challenges. In the absence of an overall approach that includes such a process, HHS faces the risk that privacy protection measures may not be consistently and effectively built into health IT programs, thus jeopardizing patient privacy as well as the public

confidence and trust that are essential to the success of a future nationwide health information network.

We are recommending that HHS include in its overall privacy approach a process for assessing and prioritizing initiatives and the stakeholders' needs to ensure that key privacy principles and challenges are completely and adequately addressed.

HHS's Assistant Secretary for Legislation provided written comments on a draft of this report. In the comments, the department generally agreed with the information provided in the draft report; however, it neither agreed nor disagreed with our recommendation. HHS agreed that more work remains to be done in the department's efforts to protect the privacy of electronic personal health information and stated that the department is actively pursuing a process for assessing and prioritizing privacy-related initiatives intended to build public trust and confidence in health IT. As we recommended, effective implementation of such a process could help ensure that the department's overall privacy approach fully addresses key privacy principles and challenges.

Background

Recognizing the potential value of IT for public and private health systems,[7] the federal government has, for several years, been working to promote the nationwide use of health IT.[8] In April 2004, President Bush called for widespread adoption of interoperable electronic health records within 10 years and issued an executive order[9] that established the position of the National Coordinator for Health IT within HHS. The National Coordinator's responsibilities include developing, maintaining, and directing the implementation of a strategic plan to guide the nationwide implementation of interoperable health IT in both the public and private sectors. According to the strategic plan, the National Coordinator is to lead efforts to build a national health IT infrastructure that is intended to, among other things, ensure that patients' individually

[7]The nation's public health system is made up of the federal, state, tribal, and local agencies that deliver health care services to and monitor the health of the population. Private health system participants include hospitals, physicians, pharmacies, nursing homes, and other organizations that deliver health care services to individual patients.

[8]Health IT is the use of technology to electronically collect, store, retrieve, and transfer clinical, administrative, and financial health information.

[9]Executive Order 13335, April 27, 2004.

identifiable health information[10] is secure, protected, and available to the patient to be used for medical and nonmedical purposes, as directed by the patient and as appropriate.

In January 2007, we reported on the steps that HHS was taking to ensure the protection of personal health information exchanged within a nationwide network and on the challenges facing health information exchange organizations in protecting electronic personal health information.[11] We reported that although HHS and the Office of the National Coordinator had initiated actions to identify solutions for protecting electronic personal health information, the department was in the early stages of its efforts and had not yet defined an overall privacy approach. As described earlier, we made recommendations regarding the need for an overall privacy approach, which we reiterated in subsequent testimonies in February 2007, June 2007, and February 2008.[12]

In our report, we described applicable provisions of HIPAA and other federal laws that are intended to protect the privacy of certain health information, along with the HIPAA Privacy Rule[13] and key principles that are reflected in the rule. Table 1 summarizes these principles.

[10]Individually identifiable health information is the term used in the Health Insurance Portability and Accountability Act of 1996 to describe "personal health information" as defined in this report.

[11]GAO-07-238.

[12]GAO, *Health Information Technology: Early Efforts Initiated, but Comprehensive Privacy Approach Needed for National Strategy*, GAO-07-400T (Washington, D.C.: Feb. 1, 2007); *Health Information Technology: Efforts Continue but Comprehensive Privacy Approach Needed for National Strategy*, GAO-07-988T (Washington, D.C.: June 19, 2007); *Health Information Technology: HHS Is Pursuing Efforts to Advance Nationwide Implementation, but Has Not Yet Completed a National Strategy*, GAO-08-499T (Washington, D.C.: Feb. 14, 2008).

[13]The Secretary of HHS issued HIPAA's Privacy Rule in December 2000, and, after modification, in August 2002. The Privacy Rule governs the use and disclosure of individually identifiable health information that, with some exceptions, is held or transmitted in any form or medium by a covered entity.

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

Principle	Description
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 is (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.

We also described in our report and testimonies challenges associated with protecting electronic health information that are faced by federal and state health information exchange organizations and health care providers. These challenges are summarized in table 2.

Table 2: Challenges to Exchanging Electronic Health Information

Challenge	Description
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.

We reported that HHS had undertaken several initiatives intended to address aspects of key principles and challenges for protecting the privacy of health information. For example, in 2005, the department awarded four health IT contracts that included requirements for developing solutions to comply with federal privacy requirements and identifying techniques and standards for securing health information.

HHS Has Taken Steps to Address Privacy Principles and Challenges, but It Has Not Fully Implemented an Overall Privacy Approach

Since January 2007, HHS has undertaken various initiatives that are contributing to its development of an overall privacy approach, although more work remains. We recommended that this overall approach include (1) identifying milestones and the entity responsible for integrating the outcomes of its privacy-related initiatives, (2) ensuring that key privacy principles in HIPAA are fully addressed, and (3) addressing key challenges associated with the nationwide exchange of health information. In this regard, the department has fulfilled the first part of our recommendation, and it has taken important steps in addressing the two other parts. Nevertheless, these steps have fallen short of fully implementing our recommendation because they do not include a process for ensuring that all key privacy principles and challenges will be fully and adequately addressed. In the absence of such a process, HHS may not be effectively positioned to ensure that health IT initiatives achieve comprehensive privacy protection within a nationwide health information network.

HHS Has Taken Steps to Address Privacy Principles and Challenges through Its Various Health IT Initiatives

The department and its Office of the National Coordinator have continued taking steps intended to address key privacy principles and challenges through various health IT initiatives. Among other things, these initiatives have resulted in technical requirements, standards, and certification criteria related to the key privacy principles described in table 1. The following are examples of ways that the Office of the National Coordinator's health IT initiatives relate to privacy principles reflected in HIPAA.

- As part of its efforts to advance health IT, the American Health Information Community[14] defines "use cases," which are descriptions of specific business processes and ways that systems should interact with users and with other systems to achieve specific goals. Among other things, several of the use cases include requirements and specifications that address aspects of the *access*, *uses and disclosures*, and *amendments* privacy principles. For example, the "consumer empowerment" use case describes at a high level specific capabilities that align with the *access* principle. It requires that health IT systems include mechanisms that allow consumers to access their own clinical information, such as lab results and

[14]The community is a federal advisory body set up to make recommendations on how to accelerate the development and adoption of health IT, including identifying health IT standards, advancing nationwide health information exchange, and protecting personal health information.

diagnosis codes, from other sources to include in their personal health records. The use case also aligns with the *uses and disclosures* principle and includes requirements that allow consumers to control access to their personal health record information and specify which information can be accessed by health care providers and organizations within health information networks. Further, the consumer empowerment use case aligns with the *amendments* privacy principle, emphasizing the need for policies to guide decisions about which data consumers should be able to modify, annotate, or request that organizations change. (Other use cases that are related to these privacy principles are the "personalized healthcare"[15] and "remote monitoring"[16] use cases.)

- Under HHS's initiative to implement a nationwide health information network,[17] in January 2007, four test network implementations, or prototypes, demonstrated potential nationwide health information exchange and laid the foundation for the Office of the National Coordinator's ongoing network trial implementations. Activities within the prototypes and the trial implementations are related to privacy principles, including the *security*, *access*, *uses and disclosures*, and *administrative requirements* principles. For example, the prototypes produced specific requirements for security mechanisms (such as data access control and encryption) that address aspects of the *security* principle. Additionally, the ongoing trial implementations are guided by requirements for using personal health data intended to address the *access*, *uses and disclosures*, and *administrative requirements* principles. For example, participants in the trial implementations are to provide the capability for consumers to access information, such as registration and medication history data, from other sources to include in their personal health records, to control access to self-entered data or clinical information held in a personal health

[15]The personalized healthcare use case focuses on the exchange of genetic/genomic test information, personal and family health history, and the use of analytical tools in electronic health records to support clinical decision making.

[16]Remote monitoring refers to the ability to monitor patient information—such as physiological, diagnostic, medication tracking, and activities of daily living measurements—using the patient's electronic or personal health record.

[17]HHS's nationwide health information network initiative is managed by the Office of National Coordinator for Health IT. Building on the results of its earlier prototypes, HHS awarded contracts to nine health information exchange organizations and cooperative agreements to six additional organizations to develop trial implementations for testing real-time information exchange and interoperability (that is, the ability of two or more systems or components to exchange information and to use the information that has been exchanged). The Social Security Administration, the Departments of Defense and Veterans Affairs, and HHS's Indian Health Services are also participating in these trials.

record, and to control the types of information that can be released from personal health records for health information exchange. In addition, organizations participating in the network are required to provide system administrators the ability to monitor and audit all access to and use of the data stored in their systems.

- The Healthcare Information Technology Standards Panel continued work to "harmonize" standards directly related to several key privacy principles, primarily the *security* principle.[18] In addition, the panel developed technical guidelines that are intended to address other privacy principles, such as the *authorization* principle and the *uses and disclosures* principle. For example, the panel's guidelines specify that systems should be designed to ensure that consumers' instructions related to authorization and consent are captured, managed, and available to those requesting the health information.

- The Certification Commission for Healthcare Information Technology, which is developing and evaluating the criteria and process for certifying the functionality, security, and interoperability of electronic health records, took steps that primarily address the *security* principle. For example, the commission defined specific security criteria for both ambulatory and inpatient electronic health records that require various safeguards to be in place before electronic health record systems are certified. Among other things, these safeguards include ensuring that system administrators can modify the privileges of users so that only those who have a need to access patients' information are allowed to do so and that the minimum amount of information necessary can be accessed by system users.

- The State-Level Health Information Exchange Consensus Project, a consortium of public and private-sector stakeholders, is intended to promote consistent organizational policies regarding privacy and health information exchange. The consortium issued a report in February 2007 that addresses, among other principles, the *uses and disclosures* privacy principle. For example, the report advises health information exchange organizations to maintain information about access to and disclosure of patients' personal health information and to make that data available to patients. The consortium subsequently issued another report in March 2008 that recommended practices to ensure the appropriate access, use, and control of health information.

[18]"Harmonizing" is the process of identifying overlaps and gaps in relevant standards and developing recommendations to address these overlaps and gaps.

Additionally, two of HHS's key advisory groups continued to develop and provide recommendations to the Secretary of HHS for addressing privacy issues and concerns:

- The Confidentiality, Privacy, and Security Workgroup was formed in 2006 by the American Health Information Community to focus specifically on these issues and has submitted recommendations to the community that address privacy principles. Among these are recommendations related to the *notice* principle that the workgroup submitted in February and April 2008. These recommendations stated that health information exchange organizations should provide patients, via the Web or another means, information in plain language on how these organizations use and disclose health information, their privacy policies and practices, and how they safeguard patient or consumer information. The work group also submitted recommendations related to the *administrative requirements* principle, stating that the obligation to provide individual rights and a notice of privacy practices under HIPAA should remain with the health care provider or plan that has an established, independent relationship with a patient, not with the health information exchange.

- The National Committee on Vital and Health Statistics, established in 1949, advises the Secretary of HHS on issues including the implementation of health IT standards and safeguards for protecting the privacy of personal health information.[19] The committee's recent recommendations related to HHS's health IT initiatives addressed, among others, the *uses and disclosures* principle. For example, in February 2008, the National Committee submitted five recommendations to the Secretary that support an individual's right to control the disclosure of certain sensitive health information for the purposes of treatment.

Although the recommendations from these two advisory groups are still under consideration by the Secretary, according to HHS officials, contracts for the nationwide health information network require participants to consider these recommendations when conducting network trials once they are accepted by the Secretary.

[19]The National Committee on Vital and Health Statistics was established 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.

The Office of the National Coordinator also took actions intended to address key challenges to protecting exchanges of personal electronic health information. Specifically, state-level initiatives (described below) were formed to bring stakeholders from states together to collaborate, propose solutions, and make recommendations to state and federal policymakers for addressing challenges to protecting the privacy of electronic personal health information within a nationwide health information exchange. Outcomes of these initiatives provided specific state-based solutions and recommendations for federal policy and guidance for addressing key challenges described by our prior work (see table 2).[20]

- The Health Information Security and Privacy Collaboration is pursuing privacy and security projects directly related to several of the privacy challenges identified in our prior work, including the need to resolve legal and policy issues resulting from varying state laws and organizational-level business practices and policies, and the need to obtain individuals' consent for the use and disclosure of personal health information. For example, the state teams noted the need for clarification about how to interpret and apply the "minimum necessary" standard, and they recommended that HHS provide additional guidance to clarify this issue. In addition, most of the state teams cited the need for a process to obtain patient permission to use and disclose personal health information, and the teams identified multiple solutions to address differing definitions of patient permission, including the creation of a common or uniform permission form for both paper and electronic environments.

- The State Alliance for e-Health created an information protection task force that in August 2007 proposed five recommendations that are intended to address the challenge of understanding and resolving legal and policy issues. The recommendations, which the alliance accepted, focused on methods to facilitate greater state-federal interaction related to protecting privacy and developing common solutions for the exchange of electronic health information.

[20]A third state-level initiative, the State-Level Health Information Exchange Consensus Project (described earlier), issued a report in March 2008 that also discusses internal challenges facing state health IT organizations, such as organizational structure and resource sustainability.

Beyond the initiatives previously discussed, in June 2008, the Secretary released a federal health IT strategic plan[21] that includes a privacy and security objective for each of its strategic goals, along with strategies and target dates for achieving the objectives. [22] For example, one of the strategies is to complete the development of a confidentiality, privacy, and security framework by the end of 2008, and another is to address inconsistent statutes or regulations for the exchange of electronic health information by the end of 2011. The strategic plan emphasized the importance of privacy protection for electronic personal health information by acknowledging that the success of a nationwide, interoperable health IT infrastructure in the United States will require a high degree of public confidence and trust.

In accordance with this strategy, the Office of the National Coordinator is responsible for developing the confidentiality, privacy, and security framework. The National Coordinator has indicated that this framework, which is to be developed and published by the end of calendar year 2008,[23] is to incorporate the outcomes of the department's privacy-related initiatives, and that milestones have been developed and responsibility assigned for integrating these outcomes. The National Coordinator has assigned responsibility for these integration efforts and the development of the framework to the Director of the Office of Policy and Research within the Office of the National Coordinator. In this regard, the department has fulfilled the first part of our recommendation.

Steps Taken Have Not Fully Implemented an Overall Privacy Approach

While the various initiatives that HHS has undertaken are contributing to the development and implementation of an overall privacy approach, more work remains. In particular, the department has not defined a process for ensuring that all privacy principles and challenges will be fully and

[21]HHS, Office of the National Coordinator for Health Information Technology, *The ONC-Coordinated Federal Health IT Strategic Plan: 2008-2012* (Washington, D.C.: June 3, 2008).

[22]The two goals defined in the strategic plan are to (1) enable the transformation to higher quality, more efficient, patient-focused health care through electronic health information access and use by care providers and by patients and their designees; and (2) enable the appropriate, authorized, and timely access and use of electronic health information to benefit public health, biomedical research, quality improvement, and emergency preparedness.

[23]The outcomes of these initiatives are also to be integrated into the development of the nationwide health information network.

adequately addressed. This process would include, for example, steps for ensuring that all stakeholders' contributions to defining privacy-related activities are appropriately considered and that individual inputs to the privacy framework will be effectively assessed and prioritized to achieve comprehensive coverage of all key privacy principles and challenges.

Such a process is important given the large number and variety of activities being undertaken and the many stakeholders contributing to the health IT initiatives. In particular, the contributing activities involve a wide variety of stakeholders, including federal, state and private-sector entities. Further, certain privacy-related activities are relevant only to specific principles or challenges, and are generally not aimed at comprehensively addressing all privacy principles and challenges. For example, the certification and standards harmonization efforts primarily address the implementation of technical solutions for interoperable health IT and, therefore, are aimed at system-level security measures, such as data encryption and password protections, while the recommendations submitted by HHS's advisory committees and state-level initiatives are primarily aimed at policy and legal issues. Effectively assessing the contributions of individual activities could play an important role in determining how each activity contributes to the collective goal of ensuring comprehensive privacy protection. Additionally, the outcomes of the various activities may address privacy principles and challenges to varying degrees. For example, while a number of the activities address the *uses and disclosures* principle, HHS's advisory committees have made recommendations that the department's activities more extensively address the *notice* principle. Consequently, without defined steps for thoroughly assessing the contributions of the activities, some principles and challenges may be addressed extensively, while others may receive inadequate attention, leading to gaps in the coverage of the principles and challenges.

In discussing this matter with us, officials in the Office of the National Coordinator pointed to the various health IT initiatives as an approach that it is taking to manage privacy-related activities in a coordinated and integrated manner. For example, the officials stated that the purpose of the American Health Information Community's use cases is to provide guidance and establish requirements for privacy protections that are intended to be implemented throughout the department's health IT initiatives (including standards harmonization, electronic health records certification, and the nationwide health information network). Similarly, contracts for the nationwide health information network require participants to adopt approved health IT standards (defined by the

Healthcare Information Technology Standards Panel) and, as mentioned earlier, to consider recommendations from the American Health Information Community and the National Committee on Vital and Health Statistics when conducting network trials, once these recommendations are accepted or adopted by the Secretary.

While these are important activities for addressing privacy, they do not constitute a defined process for assessing and prioritizing the many privacy-related initiatives and the needs of stakeholders to ensure that privacy issues and challenges will be addressed fully and adequately. Without a process that accomplishes this, HHS faces the risk that privacy protection measures may not be consistently and effectively built into health IT programs, thus jeopardizing patient privacy as well as the public confidence and trust that are essential to the success of a future nationwide health information network.

Conclusions

HHS and its Office of the National Coordinator for Health IT intend to address key privacy principles and challenges through integrating the privacy-related outcomes of the department's health IT initiatives. Although it has established milestones and assigned responsibility for integrating these outcomes and for the development of a confidentiality, privacy, and security framework, the department has not fully implemented our recommendation for an overall privacy approach that is essential to ensuring that privacy principles and challenges are fully and adequately addressed. Unless HHS's privacy approach includes a defined process for assessing and prioritizing the many privacy-related initiatives, the department may not be able to ensure that key privacy principles and challenges will be fully and adequately addressed. Further, stakeholders may lack the overall policies and guidance needed to assist them in their efforts to ensure that privacy protection measures are consistently built into health IT programs and applications. As a result, the department may miss an opportunity to establish the high degree of public confidence and trust needed to help ensure the success of a nationwide health information network.

Recommendation for Executive Action

To ensure that key privacy principles and challenges are fully and adequately addressed, we recommend that the Secretary of Health and Human Services direct the National Coordinator for Health IT to include in the department's overall privacy approach a process for assessing and prioritizing its many privacy-related initiatives and the needs of stakeholders.

Agency Comments and Our Evaluation

HHS's Assistant Secretary for Legislation provided written comments on a draft of this report. In the comments, the department generally agreed with the information discussed in our report; however, it neither agreed nor disagreed with our recommendation.

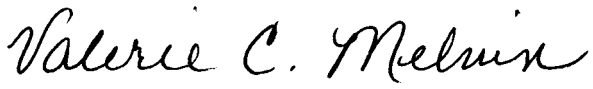
HHS agreed that more work remains to be done in the department's efforts to protect the privacy of electronic personal health information and stated that it is actively pursuing a two-phased process for assessing and prioritizing privacy-related initiatives intended to build public trust and confidence in health IT, particularly in electronic health information exchange. According to HHS, the process will include work with stakeholders to ensure that real-world privacy challenges are understood. In addition, the department stated that the process will assess the results and recommendations from the various health IT initiatives and measure progress toward addressing privacy-related milestones established by the health IT strategic plan. As we recommended, effective implementation of such a process could help ensure that the department's overall privacy approach fully addresses key privacy principles and challenges.

HHS also provided technical comments, which we have incorporated into the report as appropriate. The department's written comments are reproduced in appendix II.

We are sending copies of this report to interested congressional committees and to the Secretary of HHS. Copies of this report will 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) 512-6304 or Linda Koontz at (202) 512-6240, or by e-mail at melvinv@gao.gov or koontzl@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 III.

Sincerely yours,



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

Linda D. Koontz
Director, Information Management Issues

Appendix I: Objective, Scope, and Methodology

Our objective was to provide an update on the department's efforts to define and implement an overall privacy approach, as we recommended in an earlier report.[1] Specifically, we recommended that the Secretary of Health and Human Services define and implement an overall approach for protecting health information that would (1) identify milestones and the entity responsible for integrating the outcomes of its privacy-related initiatives, (2) ensure that key privacy principles in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) are fully addressed, and (3) address key challenges associated with the nationwide exchange of health information.

To determine the status of HHS's efforts to develop an overall privacy approach, we analyzed the department's federal health IT strategic plan and documents related to its planned confidentiality, privacy, and security framework. We also analyzed plans and documents that described activities of each of the health IT initiatives under the Office of the National Coordinator and identified those intended to (1) develop and implement mechanisms for addressing privacy principles and (2) develop recommendations for overcoming challenges to ensuring the privacy of patients' information. Specifically, we assessed descriptions of the intended outcomes of the office's health IT initiatives to determine the extent to which they related to these privacy principles and challenges identified by our prior work.

To supplement our data collection and analysis, we conducted interviews with officials from the Office of the National Coordinator to discuss the department's approaches and future plans for addressing the protection of personal health information within a nationwide health information network.

We conducted this performance audit at the Department of Health and Human Services in Washington, D.C., from April 2008 through September 2008, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

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

Appendix II: Comments from the Department of Health and Human Services

Legislation

DEPARTMENT OF HEALTH & HUMAN SERVICES OFFICE OF THE SECRETARY

Assistant Secretary for

Washington, DC 20201

SEP 11 2008

Valerie C. Melvin
Director, Human Capital and Management Information Systems
U.S. Government Accountability Office
441 G Street N.W.
Washington, DC 20548

Dear Ms. Melvin:

Enclosed are comments on the U.S. Government Accountability Office's (GAO) report entitled: "Health Information Technology: HHS Has Taken Important Steps to Address Privacy Principles and Challenges, Although More Work Remains" (GAO 08-1138).

The Department appreciates the opportunity to review this report before its publication.

Sincerely,

for Vincent J. Ventimiglia, Jr.
Assistant Secretary for Legislation

Attachment

COMMENTS OF THE DEPPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE U.S. GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO) DRAFT REPORT ENTITLED: HEALTH INFORMATION TECHNOLOGY – HHS HAS TAKEN IMPORTANT STEPS TO ADDRESS PRIVACY PRINCIPLES AND CHALLENGES, ALTHOUGH MORE WORK REMAINS (GAO 08-1138)

General Comments:

The Department of Health and Human Services (HHS) appreciates the opportunity to review the Government Accountability Office's (GAO) draft report entitled "HEALTH INFORMATION TECHNOLOGY – HHS Has Taken Important Steps to Address Privacy Principles and Challenges, Although More Work Remains."

In this update to the GAO's previous report on this subject, we appreciate the GAO's recognition that "HHS has taken important steps to address privacy principles and challenges" related to health information technology (health IT). We agree that more work remains.

Progress is being made toward the President's goal that most Americans have secure electronic health records by 2014. HHS will continue to address privacy and security from both a technology and policy perspective as we advance a nationwide, interoperable health IT infrastructure that has sufficient flexibility to be able to incorporate privacy and security solutions as they are developed.

The GAO correctly identifies many ongoing HHS initiatives that address privacy and security. It is important to note that the report lists representative examples of HHS initiatives in this area, and is not intended to provide a complete compilation of HHS's privacy and security activities.

In June 2008, HHS published the *ONC-Coordinated Federal Health IT Strategic Plan: 2008-2012* (the Strategic Plan), which includes several specific strategies to address privacy and security of personal health information in health IT initiatives. The key concept of coordination reflected in the Strategic Plan's title is an essential component of all our privacy and security strategies. While HHS is a leader in health care and health IT, we recognize that our mission cannot be accomplished without coordination and input from a wide range of stakeholders. To that end, HHS has joined with state and other Federal agencies, as well as the private sector, to engage a variety of stakeholders in our health IT initiatives. Some examples of HHS's privacy and security initiatives and activities include the Healthcare Information Technology Standards Panel, the Certification Commission for Healthcare Information Technology, the Health Information Security and Privacy Collaboration, the State Alliance for e-Health, the State-level Health Information Exchange Consensus Project, the Nationwide Health Information Network Trial Implementations, the American Health Information Community, and the National Committee on Vital and Health Statistics. Thousands of participants are engaged in these efforts.

HHS is actively pursuing a two-stage process for assessing and prioritizing privacy and security-related initiatives to build public trust and confidence in health IT and in particular electronic health information exchange. This process reflects our role as coordinators and our belief that public-private dialogue is necessary to inform next steps and achieve trust. First, we work with stakeholders to understand concerns and real-world privacy and security challenges. Second, we address privacy principles and challenges by assessing results and recommendations from our

1

COMMENTS OF THE DEPPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE U.S. GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO) DRAFT REPORT ENTITLED: HEALTH INFORMATION TECHNOLOGY – HHS HAS TAKEN IMPORTANT STEPS TO ADDRESS PRIVACY PRINCIPLES AND CHALLENGES, ALTHOUGH MORE WORK REMAINS (GAO 08-1138)

initiatives, evaluating how each activity builds on or influences the others, and measuring progress toward the milestones established in the Strategic Plan. The process has and will continue to address key privacy principles and challenges, develop policies and guidance needed by stakeholders, and build a nationwide, interoperable health IT infrastructure that includes the privacy and security protections needed to ensure public confidence and trust.

HHS initiatives will continue to assure that electronic health information is private and secure while concurrently improving individual and population health through the advancement and adoption of interoperable health IT.

2

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Valerie C. Melvin, (202) 512-6304 or melvinv@gao.gov
Linda D. Koontz, (202) 512-6240 or koontzl@gao.gov

Acknowledgments

In addition to those named above, key contributors to this report were John A. de Ferrari, Assistant Director; Teresa F. Tucker, Assistant Director; Barbara Collier; Heather A. Collins; Susan S. Czachor; Amanda C. Gill; Nancy Glover; M. Saad Khan; Thomas E. Murphy; and Sylvia L. Shanks.

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 "E-mail 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, DC 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

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548