United States Government Accountability Office

GAO

Testimony

Before the Committee on Health, Education, Labor, and Pensions

U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EST
January 15, 2009

HEALTH INFORMATION TECHNOLOGY

Federal Agencies' Experiences Demonstrate Challenges to Successful Implementation

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

January 15, 2009

HEALTH INFORMATION TECHNOLOGY

Federal Agencies' Experiences Demonstrate Challenges to Successful Implementation

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-09-312T, a hearing before the Senate Committee on Health, Education, Labor, and Pensions.

Why GAO Did This Study

As GAO and others have reported, the use of information technology (IT) has enormous potential to help improve the quality of health care and is important for improving the performance of the U.S. health care system. Given its role in providing health care, the federal government has been urged to take a leadership role to improve the quality and effectiveness of health care, and it has been working to promote the nationwide use of health IT for a number of years. However, achieving widespread adoption and implementation of health IT has proven challenging, and the best way to accomplish this transition remains subject to much debate.

At the committee's request, this testimony discusses important issues identified by GAO's work that have broad relevance to the successful implementation of health IT to improve the quality of health care.

To develop this testimony, GAO relied largely on its previous work on federal health IT activities.

What GAO Found

Health IT has the potential to help improve the efficiency and quality of health care, but achieving the transition to a nationwide health IT capability is an inherently complex endeavor. A successful transition will require, among other things, addressing the following issues:

- *Establishing a foundation of clearly defined health IT standards that are agreed upon by all important stakeholders.* Developing, coordinating, and agreeing on standards are crucial for allowing health IT systems to work together and to provide the right people access to the information they need: for example, technology standards must be agreed on (such as file types and interchange systems), and a host of content issues must also be addressed (one example is the need for consistent medical terminology). Although important steps have been taken, additional effort is needed to define, adopt, and implement such standards to promote data quality and consistency, system interoperability (that is, the ability of automated systems to share and use information), and information protection.

- *Defining comprehensive plans that are grounded in results-oriented milestones and measures.* Using interoperable health IT to improve the quality and efficiency of health care is a complex goal that involves a range of stakeholders, various technologies, and numerous activities taking place over an expanse of time, and it is important that these activities be guided by comprehensive plans that include milestones and performance measures. Without such plans, it will be difficult to ensure that the many activities are coordinated, their results monitored, and their outcomes most effectively integrated.

- *Implementing an approach to protection of personal privacy that encourages public acceptance of health IT.* A robust approach to privacy protection is essential to establish the high degree of public confidence and trust needed to encourage widespread adoption of health IT and particularly electronic medical records. Health IT programs and applications need to address key privacy principles (for example, the access principle, which establishes the right of individuals to review certain personal health information). At the same time, they need to overcome key challenges (for example, those related to variations in states' privacy laws). Unless these principles and challenges are fully and adequately addressed, there is reduced assurance that privacy protection measures will be consistently built into health IT programs and applications, and public acceptance of health IT may be put at risk.

To view the full product, including the scope and methodology, click on GAO-09-312T. For more information, contact Valerie Melvin at (202) 512-6304 or melvinv@gao.gov.

Mr. Chairman and Members of the Committee:

I am pleased to be here today to comment on federal efforts to advance the use of health information technology (IT). Studies published by the Institute of Medicine and others have long indicated that fragmented, disorganized, and inaccessible clinical information adversely affects the quality of health care and compromises patient safety. Further, long-standing problems with medical errors and inefficiencies have contributed to increased costs of health care. With health care spending in 2007 reaching approximately $2.2 trillion, or 16 percent of the U.S. gross domestic product, concerns about the costs of health care have continued to grow, and have prompted calls from policy makers, industry experts, and medical practitioners to improve the U.S. health care system.

As has been recognized by you and other members of Congress, as well as President Bush and President-elect Obama, the use of information technology to electronically collect, store, retrieve, and transfer clinical, administrative, and financial health information has great potential to help improve the quality and efficiency of health care. The successful implementation of health IT offers promise for improving patient safety and reducing inefficiencies and has been shown to support cost savings and other benefits. At the same time, successfully achieving widespread adoption and implementation of health IT has proven challenging, and the best way to accomplish this goal remains subject to much debate. According to the Department of Health and Human Services (HHS), only a small number of U.S. health care providers have fully adopted health IT due to significant financial, technical, cultural, and legal barriers, such as a lack of access to capital, a lack of data standards, and resistance from health care providers.

Given its role in providing health care, the federal government has been urged to take a leadership role to improve the quality and effectiveness of health care and has been working to promote the nationwide use of health IT for a number of years. In April 2004, President Bush issued an executive order that called for widespread

adoption of interoperable electronic health records by 2014,[1] and HHS, in turn, initiated activities to advance the nationwide implementation of interoperable health IT. In addition, for the past decade, the Departments of Defense (DOD) and Veterans Affairs (VA) have been pursuing initiatives to share data between their health information systems. In an effort to expedite the exchange of electronic health information between the two departments, the National Defense Authorization Act for Fiscal Year 2008[2] included provisions directing the two departments to jointly develop and implement, by September 30, 2009, fully interoperable[3] electronic health record systems or capabilities.

Since 2001, we have been reviewing aspects of the various federal efforts undertaken to implement information technology for health care and public health solutions. We have reported both on HHS's national health IT initiatives as well as on DOD's and VA's electronic health information sharing initiatives.[4] Overall, our studies have recognized progress made by these departments, but we have also pointed out areas of concern that could jeopardize their success in advancing the use of interoperable health IT. At your request, my testimony today discusses important issues identified by our work

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

[2]Pub. L. No. 110-181, § 1635 (2008).

[3]Interoperability is the ability of two or more systems or components to exchange information and to use the information that has been exchanged.

[4]GAO, *Computer-Based Patient Records: Better Planning and Oversight by VA, DOD, and IHS Would Enhance Health Data Sharing*, GAO-01-459 (Washington, D.C.: Apr. 30, 2001); *Computer-Based Patient Records: VA and DOD Efforts to Exchange Health Data Could Benefit from Improved Planning and Project Management*, GAO-04-687 (Washington, D.C.: June 7, 2004); *Health Information Technology: HHS Is Taking Steps to Develop a National Strategy*, GAO-05-628 (Washington, D.C.: May 27, 2005); *Health Information Technology: HHS Is Continuing Efforts to Define its National Strategy*, GAO-06-1071T (Washington, D.C.: Sept. 1, 2006); *Information Technology: DOD and VA Have Increased Their Sharing of Health Information, but More Work Remains*, GAO-08-954 (Washington, D.C.: July 28, 2008); *Health Information Technology: HHS Has Taken Important Steps to Address Privacy Principles and Challenges, Although More Work Remains*, GAO-08-1138 (Washington, D.C.: Sept. 17, 2008); and *Electronic Health Records: DOD and VA Have Increased Their Sharing of Health Information, but Further Actions Are Needed*, GAO-08-1158T (Washington, D.C.: Sept. 24, 2008).

that have broad relevance to the successful implementation of health IT to further improve the quality of health care.

In developing this testimony, we relied largely on our previous work. We conducted our work in support of this testimony between December 2008 and January 2009 in Washington, D.C. All work on which this testimony is based was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits 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.

In summary, transitioning to a nationwide health IT capability is an inherently complex endeavor. Achieving this transition and the potential efficiencies and quality improvements promised by widespread adoption of health IT will require consideration of many serious issues, including the need for a foundation of clearly defined health IT standards that are agreed upon by all important stakeholders, comprehensive planning grounded in results-oriented milestones and measures, and an approach to privacy protection that encourages acceptance and adoption of electronic health records.

- Developing, coordinating, and agreeing on standards are crucial for allowing health IT systems to work together and to provide the right people access to the information they need. Any level of interoperability depends on the use of agreed-upon standards to ensure that information can be shared and used. Developing and implementing health IT standards requires structures and ongoing mechanisms that include the participation of the relevant stakeholders, in both the public and private health care sectors who will be sharing information. Although important steps have been taken, additional effort is needed to define, adopt, and implement such standards to promote data quality and consistency, system interoperability, and information protection.

- Using interoperable health IT to improve the quality and efficiency of health care is a complex goal that involves a range of

stakeholders, various technologies, and numerous activities taking place over an expanse of time; in view of this complexity, it is important that these activities be guided by comprehensive plans that include milestones and performance measures. Milestones and performance measures allow the results of the activities to be monitored and assessed, so that corrective action can be taken if needed. Without comprehensive plans, it will be difficult to ensure that the many activities are coordinated, their results monitored, and their outcomes integrated.

- An important consideration in health IT is an overall approach for protecting the privacy of personal electronic health information. 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. Addressing and mitigating this risk is essential to encourage public acceptance of the increased use of health IT and electronic medical records. We have identified[5] key privacy principles that health IT programs and applications need to address[6] and key challenges that they need to overcome.[7] Unless these principles and challenges are fully and adequately addressed, there is reduced assurance that privacy protection measures will be

[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]We based these privacy principles on our evaluation of the HHS Privacy Rule promulgated under the Administrative Simplification 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. For example, the uses and disclosures principle provides, among other things, limits to the circumstances in which an individual's protected heath information may be used or disclosed by covered entities, and the access principle establishes individuals' rights to review and obtain a copy of their protected health information held in a designated record set. For more details, see GAO-07-238.

[7]We identified key challenges associated with protecting personal health information based on input from selected stakeholders in health information exchange organizations. These challenges are understanding and resolving legal and policy issues (for example, 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. See GAO-07-238.

consistently built into health IT programs and applications, and public acceptance of health IT may be put at risk.

Background

Health care in the United States is a highly decentralized system, with stakeholders that include not only the entire population as consumers of health care, but also all levels of government, health care providers such as medical centers and community hospitals, patient advocates, health professionals, major employers, nonprofit health organizations, insurance companies, commercial technology providers, and others. In this environment, clinical and other health-related information is stored in a complex collection of paper files, information systems, and organizations, but much of it continues to be stored and shared on paper.

Successfully implementing health IT to replace paper and manual processes has been shown to support benefits in both cost savings and improved quality of care. For example, we reported to this committee in 2003[8] that a 1,951-bed teaching hospital stated that it had realized about $8.6 million in annual savings by replacing outpatient paper medical charts with electronic medical records. This hospital also reported saving more than $2.8 million annually by replacing its manual process for managing medical records with an electronic process to provide access to laboratory results and reports. Other technologies, such as bar coding of certain human drug and biological product labels, have also been shown to save money and reduce medical errors. 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.

There is also potential benefit from improving and expanding existing health IT systems. We have reported that some hospitals are

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

expanding their IT systems to support improvements in quality of care. In April 2007,[9] we released a study on the processes used by eight hospitals to collect and submit data on their quality of care to HHS's Centers for Medicare & Medicaid Services (CMS). Among the hospitals we visited, officials noted that having electronic records was an advantage for collecting the quality data because electronic records were more accessible and legible than paper records, and the electronic quality data could also be used for other purposes (such as reminders to physicians). Officials at each of the hospitals reported using the quality data to make specific changes in their internal procedures designed to improve care. However, hospital officials also reported several limitations in their existing IT systems that constrained the ability to support the collection of their quality data. For example, hospitals reported having a mix of paper and electronic systems, having data recorded only as unstructured narrative or other text, and having multiple systems within a single hospital that could not access each other's data. Although it was expected to take several years, all the hospitals in our study were working to expand the scope and functionality of their IT systems.

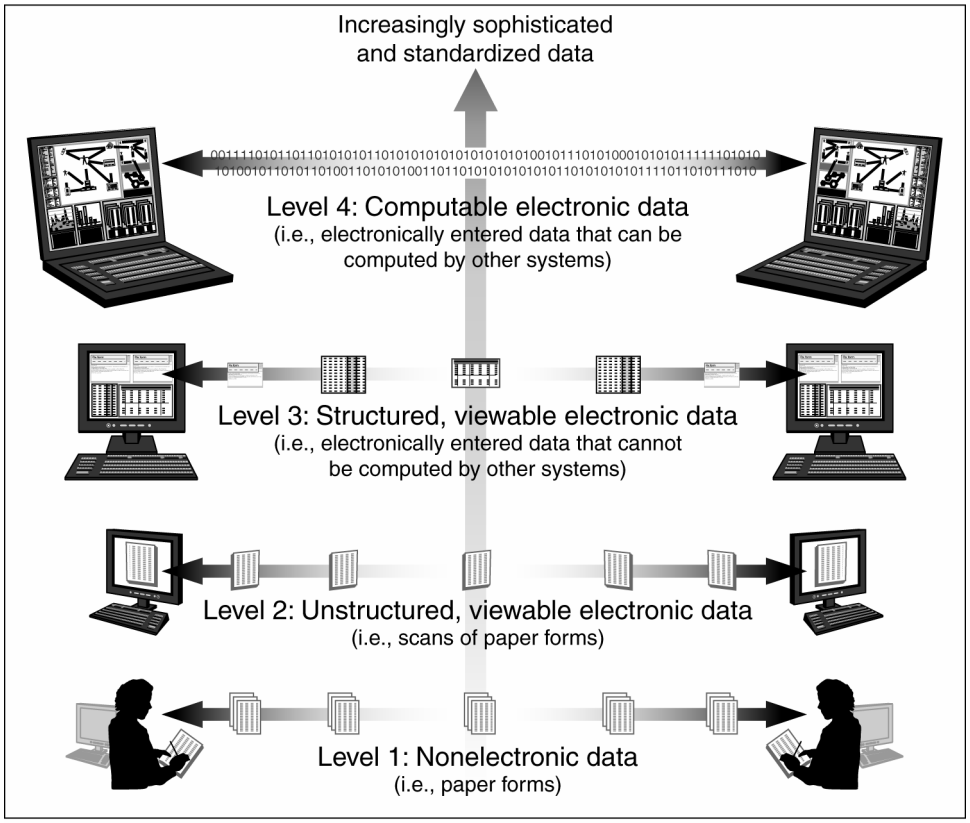
This example illustrates, among other things, that making health care information electronically available depends on interoperability—that is, the ability of two or more systems or components to exchange information and to use the information that has been exchanged. This capability is important because it allows patients' electronic health information to move with them from provider to provider, regardless of where the information originated. If electronic health records conform to interoperability standards, they can be created, managed, and consulted by authorized clinicians and staff across more than one health care organization, thus providing patients and their caregivers the necessary information required for optimal care. (Paper-based health records—if available—also provide necessary information, but unlike electronic health records, do not provide automated

[9]GAO, *Hospital Quality Data: HHS Should Specify Steps and Time Frame for Using Information Technology to Collect and Submit Data*, GAO-07-320 (Washington, D.C.: Apr. 25, 2007).

decision support capabilities, such as alerts about a particular patient's health, or other advantages of automation.)

Interoperability may be achieved at different levels (see fig. 1). For example, at the highest level, electronic data are computable (that is, in a format that a computer can understand and act on to, for example, provide alerts to clinicians on drug allergies). At a lower level, electronic data are structured and viewable, but not computable. The value of data at this level is that they are structured so that data of interest to users are easier to find. At still a lower level, electronic data are unstructured and viewable, but not computable. With unstructured electronic data, a user would have to find needed or relevant information by searching uncategorized data.

Figure 1: Levels of Data Interoperability



Source: GAO analysis based on data from the Center for Information Technology Leadership.

It is important to note that not all data require the same level of interoperability. For example, computable pharmacy and drug allergy data would allow automated alerts to help medical personnel avoid administering inappropriate drugs. On the other hand, for such narrative data as clinical notes, unstructured, viewable data may be sufficient. Achieving even a minimal level of electronic interoperability would potentially make relevant information available to clinicians.

Any level of interoperability depends on the use of agreed-upon standards to ensure that information can be shared and used. In the health IT field, standards may govern areas ranging from technical issues, such as file types and interchange systems, to content issues, such as medical terminology.

- For example, *vocabulary standards* provide common definitions and codes for medical terms and determine how information will be documented for diagnoses and procedures. These standards are intended to lead to consistent descriptions of a patient's medical condition by all practitioners. The use of common terminology helps in the clinical care delivery process, enables consistent data analysis from organization to organization, and facilitates transmission of information. Without such standards, the terms used to describe the same diagnoses and procedures may vary (the condition known as hepatitis, for example, may be described as a liver inflammation). The use of different terms to indicate the same condition or treatment complicates retrieval and reduces the reliability and consistency of data.

- Another example is *messaging standards*, which establish the order and sequence of data during transmission and provide for the uniform and predictable electronic exchange of data. These standards dictate the segments in a specific medical transmission. For example, they might require the first segment to include the patient's name, hospital number, and birth date. A series of subsequent segments might transmit the results of a complete blood count, dictating one result (e.g., iron content) per segment. Messaging standards can be adopted to enable intelligible communication between organizations via the Internet or some other communications pathway. Without them, the interoperability of health IT systems may be limited, reducing the data that can be shared.

  Developing interoperability standards requires the participation of the relevant stakeholders who will be sharing information. In the case of health IT, stakeholders include both the public and private sectors. The public health system is made up of the federal, state, tribal, and local agencies that may deliver health care services to the population and monitor its health. Private health system participants include hospitals, physicians, pharmacies, nursing homes, and other organizations that deliver health care services to individual patients, as well as multiple vendors that provide health IT solutions.

Federal Health IT Efforts Highlight Importance of Establishing Standards, Developing Comprehensive Plans, and Ensuring Privacy

Widespread adoption of health IT has the potential to improve the efficiency and quality of health care. However, transitioning to this capability is a challenging endeavor that requires attention to many important considerations. Among these are mechanisms to establish clearly defined health IT standards that are agreed upon by all important stakeholders, comprehensive planning grounded in results-oriented milestones and measures, and an approach to privacy protection that encourages acceptance and adoption of electronic health records. Attempting to expand the use of health IT without fully addressing these issues would put at risk the ultimate goal of achieving more effective health care.

Mechanisms and Structures for Harmonizing and Implementing Health IT Standards Are Essential to Enable Interoperability

The need for health care standards has been broadly recognized for a number of years. In previous work, we identified lessons learned by U.S. agencies and by other countries from their experiences. Among other lessons, they reported the need to define and adopt common standards and terminology to achieve data quality and consistency, system interoperability, and information protection.[10] In May 2003, we reported that federal agencies recognized the need for health care standards and were making efforts to strengthen and increase their use.[11] However, while they had made progress in defining standards, they had not met challenges in identifying and implementing standards necessary to support interoperability across the health care sector. We stated that until these challenges were addressed, agencies risked promulgating piecemeal and disparate systems unable to exchange data with each other when

[10]GAO, *Health Information Technology: HHS Is Taking Steps to Develop a National Strategy*, GAO-05-628 (Washington, D.C.: May 27, 2005).

[11]GAO, *Bioterrorism: Information Technology Strategy Could Strengthen Federal Agencies' Abilities to Respond to Public Health Emergencies*, GAO-03-139 (Washington, D.C.: May 30, 2003).

needed. We recommended that the Secretary of HHS define activities for ensuring that the various standards-setting organizations coordinate their efforts and reach further consensus on the definition and use of standards; establish milestones for defining and implementing standards; and create a mechanism to monitor the implementation of standards through the health care industry.

HHS implemented this recommendation through the activities of the Office of the National Coordinator for Health Information Technology (established within HHS in April 2004). Through the Office of the National Coordinator, HHS designated three primary organizations, made up of stakeholders from both the public and private health care sectors, to play major roles in identifying and implementing standards and expanding the implementation of health IT:

- The American Health Information Community (now known as the National eHealth Collaborative) was created by the Secretary of HHS to make recommendations on how to accelerate the development and adoption of health IT, including advancing interoperability, identifying health IT standards, advancing nationwide health information exchange, and protecting personal health information. Created in September 2005 as a federal advisory commission, the organization recently became a nonprofit membership organization. It includes representatives from both the public and private sectors, including high-level officials of VA and other federal and state agencies, as well as health systems, payers, health professionals, medical centers, community hospitals, patient advocates, major employers, nonprofit health organizations, commercial technology providers, and others. Among other things, the organization has identified health care areas of high priority and developed "use cases" for these areas (use cases are descriptions of events or scenarios, such as Public Health Case Reporting, that provide the context in which standards would be applicable, detailing what needs to be done to achieve a specific mission or goal).

- The Healthcare Information Technology Standards Panel (HITSP), sponsored by the American National Standards Institute[12] and funded by the Office of the National Coordinator, was established in October 2005 as a public-private partnership to identify competing standards for the use cases developed by the American Health Information Community and to "harmonize" the standards.[13] As of March 2008, nearly 400 organizations[14] representing consumers, healthcare providers, public health agencies, government agencies, standards developing organizations, and other stakeholders were participating in the panel and its committees. The panel also develops the interoperability specifications that are needed for implementing the standards. In collaboration with the National Institute for Standards and Technology, HITSP selected initial standards to address, among other things, requirements for message and document formats and for technical networking. Federal agencies that administer or sponsor federal health programs are now required to implement these standards, in accordance with an August 2006 Executive Order.[15]

- The Certification Commission for Healthcare Information Technology is an independent, nonprofit organization that certifies health IT products, such as electronic health records systems. HHS entered into a contract with the commission in October 2005 to

[12]The American National Standards Institute is a private, nonprofit organization whose mission is to promote and facilitate voluntary consensus standards and ensure their integrity.

[13]Harmonization is the process of identifying overlaps and gaps in relevant standards and developing recommendations to address these overlaps and gaps.

[14]Members include representatives from the following sectors: clinicians; providers; safety net providers and their representative organizations; vendors that develop, market, install, and support health IT products; healthcare purchasers or employers; healthcare payers or health insurance companies; public health professionals; national organizations with a broad representation of stakeholders with an interest in healthcare IT standards; clinical and health-services researchers' representative organizations; federal, state, and local agencies; coordinating bodies with responsibilities for and/or a relationship to healthcare IT used in the public sector; and consumer organizations with an interest in health IT standards.

[15]Executive Order 13410, *Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs* (Washington, D.C.: Aug. 22, 2006).

develop and evaluate the certification criteria and inspection process for electronic health records. HHS describes certification as the process by which vendors' health IT systems are established to meet interoperability standards. The certification criteria defined by the commission incorporate the interoperability standards and specifications defined by HITSP. The results of this effort are intended to help encourage health care providers throughout the nation to implement electronic health records by giving them assurance that the systems will provide needed capabilities (including ensuring security and confidentiality) and that the electronic records will work with other systems without reprogramming.[16]

The interconnected work of these organizations to identify and promote the implementation of standards is important to the overall effort to advance the use of interoperable health IT. For example, according to HHS, the HITSP standards are incorporated into the National Coordinator's ongoing initiative to enable health care entities—such as providers, hospitals, and clinical labs—to exchange electronic health information on a nationwide basis. Under this initiative, HHS awarded contracts to nine regional and state health information exchanges as part of its efforts to provide prototypes of nationwide networks of health information exchanges.[17] Such exchanges are intended to eventually form a "network of networks" that is to produce the envisioned Nationwide Health Information Network (NHIN). According to HHS, the department planned to demonstrate the experiences and lessons learned from this work in December 2008, including defining specifications based upon the work of HITSP and standards development organizations to facilitate interoperable data exchange

[16]In May 2006, HHS finalized a process and criteria for certifying the interoperability of outpatient electronic health records and described criteria for future certification requirements. Certification criteria for inpatient electronic health records were finalized in June 2007. To date, the Certification Commission reports that it has certified about 140 products offering electronic health records.

[17]These exchanges are intended to connect providers and patients from different regions of the country and enable the sharing of electronic health information, such as health records and laboratory results. DOD, VA, and the Indian Health Service are participating in a federal component of this initiative.

among the participants, testing interoperability against these specifications, and developing trust agreements among participants to protect the information exchanged. HHS plans to place the nationwide health information exchange specifications defined by the participating organizations, as well as related testing materials, in the public domain, so that they can be used by other health information exchange organizations to guide their efforts to adopt interoperable health IT.

The products of the federal standards initiatives are also being used by DOD and VA in their ongoing efforts to achieve the seamless exchange of health information on military personnel and veterans. The two departments have committed to the goal of adopting applicable current and emerging HITSP standards. According to department officials, DOD is also taking steps to ensure compliance with standards through certification. To ensure that the electronic health records produced by the department's modernized health information system, AHLTA,[18] are compliant with standards, it is arranging for certification through the Certification Commission for Healthcare Information Technology. Both departments are also participating in the National Coordinator's standards initiatives. The involvement of the departments in these activities is an important mechanism for aligning their electronic health records with emerging federal standards.

Federal efforts to implement health IT standards are ongoing and some progress has been made. However, until agencies are able to demonstrate interoperable health information exchange between stakeholders on a broader level, the overall effectiveness of their efforts will remain unclear. In this regard, continued work on standards initiatives will remain essential for extending the use of health IT and fully achieving its potential benefits, particularly as both information technology and medicine advance.

[18]AHLTA originally was an acronym for Armed Forces Health Longitudinal Technology Application. The department no longer considers AHLTA an acronym but the official name of the system.

Comprehensive Planning with Milestones and Performance Measures Is Essential to Achieving Health IT Goals

Using interoperable health IT to help improve the efficiency and quality of health care is a complex goal that involves a range of stakeholders and numerous activities taking place over an expanse of time; in view of this complexity, it is important to develop comprehensive plans that are grounded in results-oriented milestones and performance measures. Without comprehensive plans, it is difficult to coordinate the many activities under way and integrate their outcomes. Milestones and performance measures allow the results of the activities to be monitored and assessed, so that corrective action can be taken if needed.

Since it was established in 2004, the Office of the National Coordinator has pursued a number of health IT initiatives (some of which we described above), aimed at the expansion of electronic health records, identification of interoperability standards, advancement of nationwide health information exchange, and protection of personal health information.[19] It also developed a framework for strategic action for achieving an interoperable national infrastructure for health IT, which was released in 2004. We have noted accomplishments resulting from these various initiatives, but we also observed that the strategic framework did not include the detailed plans, milestones, and performance measures needed to ensure that the department integrated the outcomes of its various health IT initiatives and met its overall goals.[20] Given the many activities to be coordinated and the many stakeholders involved, we recommended in May 2005 that HHS define a national strategy for health IT that would include the necessary detailed plans, milestones, and performance measures, which are essential to help ensure progress toward the President's

[19]In prior work, we described programs that other divisions within HHS, such as the Agency for Healthcare Research and Quality and the Health Resources and Services Administration, administer to provide funding to organizations engaged in building and testing health IT systems, standards, and projects. See GAO-05-628 for a description of these activities.

[20]GAO, *Health Information Technology: HHS Is Taking Steps to Develop a National Strategy*, GAO-05-628 (Washington, D.C.: May 27, 2005).

goal for most Americans to have access to interoperable electronic health records by 2014. The department agreed with our recommendation, and in June 2008 it released a four-year strategic plan. If the plan's milestones and measures for achieving an interoperable nationwide infrastructure for health IT are appropriate and properly implemented, the plan could help ensure that HHS's various health IT initiatives are integrated and provide a useful roadmap to support the goal of widespread adoption of interoperable electronic health records.[21]

Across our health IT work at HHS and elsewhere, we have seen other instances in which planning activities have not been sufficiently comprehensive. An example is the experience of DOD and VA, which have faced considerable challenges in project planning and management in the course of their work on the seamless exchange of electronic health information. As far back as 2001 and 2002, we noted management weaknesses, such as inadequate accountability and poor planning and oversight, and recommended that the departments apply principles of sound project management.[22] The departments' efforts to meet the recent requirements of the National Defense Authorization Act for Fiscal Year 2008 provide additional examples of such challenges, raising concerns regarding their ability to meet the September 2009 deadline for developing and implementing interoperable electronic health record systems or capabilities. In July 2008, we identified steps that the departments had taken to establish an interagency program office and implementation plan, as required. According to the departments, they intended the program office to play a crucial role in accelerating efforts to achieve electronic health records and capabilities that allow for full interoperability, and they had

[21]In another example, as a result of the 2007 study of hospital quality data collection mentioned earlier, we recommended that the Secretary of HHS identify the specific steps that the department planned to take to promote the use of health IT for the collection and submission of these data, and that it inform interested parties of those steps and the expected time frame, including milestones for completing them.

[22]GAO, *Computer-Based Patient Records: Better Planning and Oversight by VA, DOD, and IHS Would Enhance Health Data Sharing*, GAO-01-459 (Washington, D.C.: Apr. 30, 2001) and *Veterans Affairs: Sustained Management Attention Is Key to Achieving Information Technology Results*, GAO-02-703 (Washington, D.C.: June 12, 2002).

appointed an Acting Director from DOD and an Acting Deputy Director from VA. According to the Acting Director, the departments also have detailed staff and provided temporary space and equipment to a transition team. However, the newly established program office was not expected to be fully operational until the end of 2008—allowing the departments at most 9 months to meet the deadline for full interoperability.

Further, we reported other planning and management weaknesses. For example, the departments developed a DOD/VA Information Interoperability Plan in September 2008, which is intended to address interoperability issues and define tasks required to guide the development and implementation of an interoperable electronic health record capability. Although the plan included milestones and schedules, it was lacking many milestones for completing the activities defined in the plan. Accordingly, we recommended that the departments give priority to fully establishing the interagency program office and finalizing the implementation plan. Without an effective plan and a program office to ensure its implementation, the risk is increased that the two departments will not be able to meet the September 2009 deadline.

Establishing a Consistent Approach to Privacy Protection Is Essential for Encouraging Acceptance and Adoption of Health IT

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. Addressing and mitigating this risk is essential to encourage public acceptance of the increased use of health IT and electronic medical records.

Recognizing the importance of privacy protection, HHS included security and privacy measures in its 2004 framework for strategic action, and in September 2005, it awarded a contract to the Health Information Security and Privacy Collaboration as part of its efforts to provide a nationwide synthesis of information to inform privacy

and security policymaking at federal, state, and local levels. The collaboration 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. As a result of this work, HHS developed and made available to the public a toolkit to guide health information exchange organizations in conducting assessments of business practices, policies, and state laws that govern the privacy and security of health information exchange.[23]

However, we reported in January 2007 that HHS initiated these and other important privacy-related efforts[24] without first defining an overall approach for protecting privacy. In our report, we identified key privacy principles and challenges to protecting electronic personal health information.

- Examples of principles that health IT programs and applications need to address include the uses and disclosures principle, which provides limits to the circumstances in which an individual's protected heath information may be used or disclosed, and the access principle, which establishes individuals' rights to review and obtain a copy of their protected health information in certain circumstances.[25]

[23]In June 2007, HHS reported the outcomes of its privacy and security solutions contract based on the work of 34 states and territories that participated in the contract. A final summary report described variations among organization-level business practices, policies, and laws for protecting health information that could affect organizations' abilities to exchange data.

[24]Our January 2007 report (GAO-07-238) describes various privacy-related efforts incorporated into HHS's overall health IT initiative, including the activities of the American Health Information Community, the Healthcare Information Technical Standards Panel, the Certification Commission for Healthcare IT, and the Nationwide Health Information Network.

[25]We based these privacy principles on our evaluation of the HHS Privacy Rule promulgated under the Administrative Simplification 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.

- Key challenges include understanding and resolving legal and policy issues (for example, 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.[26]

  We recommended that HHS define and implement an overall privacy approach that identifies milestones for integrating the outcomes of its privacy-related initiatives, ensures that key privacy principles are fully addressed, and addresses challenges associated with the nationwide exchange of health information.

  In September 2008, we reported that HHS had begun to establish an overall approach for protecting the privacy of personal electronic health information—for example, it had identified milestones and an entity responsible for integrating the outcomes of its many privacy-related initiatives.[27] Further, the federal health IT strategic plan released in June 2008 includes privacy and security objectives along with strategies and target dates for achieving them.

  However, in our view, more actions are needed. Specifically, within its approach, the department had not defined a process to ensure that the key privacy principles and challenges we had identified were fully and adequately addressed. This process should 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 are effectively assessed and prioritized to achieve comprehensive coverage of all key privacy principles and challenges. Without such a process, stakeholders may lack the overall policies and guidance needed to assist them in their efforts to ensure that privacy protection

[26]We identified key challenges associated with protecting personal health information based on input from selected stakeholders in health information exchange organizations.

[27]GAO, *Health Information Technology: HHS Has Taken Important Steps to Address Privacy Principles and Challenges, Although More Work Remains*, GAO-08-1138 (Washington, D.C.: Sept. 17, 2008).

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. To address these concerns, we recommended in our September report that HHS include in its overall privacy approach a process for ensuring that key privacy principles and challenges are completely and adequately addressed.

Lacking an overall approach for protecting the privacy of personal electronic health information, there is reduced assurance that privacy protection measures will be consistently built into health IT programs and applications. Without such assurance, public acceptance of health IT may be at risk.

In closing, Mr. Chairman, many important steps have been taken, but more is needed before we can make a successful transition to a nationwide health IT capability and take full advantage of potential improvements in care and efficiency that this could enable. It is important to have structures and mechanisms to build, maintain, and expand a robust foundation of health IT standards that are agreed upon by all important stakeholders. Further, given the complexity of the activities required to implement health IT and the large number of stakeholders, completing and implementing comprehensive planning activities are also key to ensuring program success. Finally, an overall privacy approach that ensures public confidence and trust is essential to successfully promoting the use and acceptance of health IT. Without further action taken to address these areas of concern, opportunities to achieve greater efficiencies and improvements in the quality of the nation's health care may not be realized.

This concludes my statement. I would be pleased to answer any questions that you or other Members of the Committee may have.

Contacts and Acknowledgments

If you should have any questions about this statement, please contact me at (202) 512-6304 or by e-mail at melvinv@gao.gov. Other individuals who made key contributions to this statement are Barbara S. Collier, Heather A. Collins, Amanda C. Gill, Linda T. Kohn, Rebecca E. LaPaze, and Teresa F. Tucker.