GAO

For Release on Delivery
2:00 p.m. EDT July 14, 2004

HEALTH CARE

National Strategy Needed to Accelerate the Implementation of Information Technology

Statement of David A. Powner,
Director, Information Technology Management Issues

G A O
Accountability ★ Integrity ★ Reliability

HEALTH CARE

National Strategy Needed to Accelerate the Implementation of Information Technology

Why GAO Did This Study

Health care is an information-intensive industry that remains highly fragmented and inefficient. Hence, the uses of information technology (IT)—in delivering clinical care, performing administrative functions, and supporting the public health infrastructure—have the potential to yield both cost savings and improvements in the care itself.

In 2003, GAO reported on benefits to health care that could result from using IT—both cost savings and measurable improvements in the delivery and quality of care. GAO also reported on federal agencies' existing and planned information systems intended to support our nation's preparedness for and ability to respond to public health emergencies and the status of health care standards setting initiatives.

The subcommittee has asked GAO to summarize our work on reported benefits of the use of IT for health care delivery and on IT initiatives supporting public health preparedness and response.

www.gao.gov/cgi-bin/getrpt?GAO-04-947T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact David A. Powner at 202-512-9286 or pownerd@gao.gov.

What GAO Found

The use of IT can yield benefits in clinical care and associated administrative functions as well as in public health. Health care organizations reported that electronic medical records (EMR) improved the delivery of care because, among other reasons, more complete medical documentation was available to support the provider's diagnosis. In addition, EMRs could greatly facilitate the reporting of public health information associated with the early detection of and response to disease outbreaks. One hospital replaced outpatients' paper medical charts with EMRs, realizing about $8.6 million in annual savings. This hospital also established electronic access to laboratory results and reports, replacing its manual process for handling medical records and saving another $2.8 million a year. In addition, the lessons learned that were reported to us by health care organizations that have successfully implemented solutions could be used by other organizations to accelerate the adoption of health IT. These lessons recognize the importance of reengineering business processes, gaining users' acceptance of IT, providing adequate training, and making systems secure.

Regarding public health, federal agencies identified 72 existing and planned information systems—34 surveillance systems, 18 supporting technologies, 10 communications systems, and 10 detection systems. For example, the Centers for Disease Control and Prevention is currently implementing its Public Health Information Network comprised of a number of disease surveillance and communications systems, including the Health Alert Network. This network is an early warning and response system that is intended to facilitate communication among federal, state, and local agencies during public health emergencies. GAO also reported that identification and implementation of health care data, communications, and security standards—which are necessary to support compatibility and interoperability of agencies' various IT systems—remained incomplete across the health care sector. To address the challenges of coordinating the many IT initiatives and implementing a consistent set of standards, GAO recommended last year that the Secretary of Health and Human Services develop a strategy for public health preparedness and response, to include setting priorities for IT initiatives and establishing mechanisms to monitor the implementation of standards throughout the health care industry. Since that time, progress has been made in identifying standards. The Office of Management and Budget's e-government initiative, the Consolidated Health Informatics initiative, has identified a number of standards to be applied to new federal development efforts and modifications of existing systems. This initiative is intended to promote the interoperability of information systems. However, implementing these standards across the federal government is still a work in progress. Until these standards are implemented, information-sharing challenges will remain. In April of this year, Executive Order 13335 established a National Health IT Coordinator and called for a strategic plan to guide the nationwide implementation of interoperable health IT. As this plan moves forward, it will be essential to have continued leadership, clear direction, measurable goals, and mechanisms to monitor progress.

United States General Accounting Office

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss the benefits that effective implementation of information technology (IT) can bring to the health care industry. According to the Institute of Medicine and others, health care is an information-intensive industry that remains highly fragmented and inefficient. Hence, the uses of IT—in delivering clinical care, performing administrative functions, and supporting the public health infrastructure[1]—have the potential to yield both cost savings and improvements in the care itself.

However, effectively implementing IT has historically been a major challenge for this industry. Currently there is inconsistent use of IT in exchanging data and delivering care. In addition, implementing information security measures that resist cyber attacks also remains a challenge.

At your request, today I will summarize our previously issued reports on (1) the reported benefits of using IT for health care delivery, including lessons learned from health care organizations that have implemented IT and (2) IT initiatives that support the public health infrastructure, including the status of standards setting initiatives that are necessary to support greater information sharing.[2] In preparing this testimony, we summarized our prior reports and updated progress on our recommendations in accordance with generally accepted government auditing standards.

---

[1]The public health infrastructure is the foundation that supports the planning, delivery, and evaluation of public health activities and is comprised of a well-trained workforce, effective program and policy evaluation, sufficient epidemiology and surveillance capability to detect outbreaks and monitor incidence of diseases, appropriate response capacity for public health emergencies, effective laboratories, secure information systems, and advanced communications systems.

[2]U.S. General Accounting Office, *Bioterrorism: Information Technology Strategy Could Strengthen Federal Agencies' Abilities to Respond to Public Health Emergencies*, GAO-03-139 (Washington, D.C.: May 30, 2003) and U.S. General Accounting Office, *Information Technology: Benefits Realized for Selected Health Care Functions,* GAO-04-224 (Washington, D.C.: October 31, 2003).

Results in Brief

As we reported last year, cost savings and other benefits realized by health care organizations that have implemented IT can be significant both in providing clinical health care and in performing the administrative functions associated with health care delivery. For example, using bar code technology and wireless scanners to verify both the identities of patients and their correct medications, a community hospital prevented the administration of over 1,200 wrong drugs or dosages and almost 2,000 early or extra doses. The monetary value of the errors that were prevented was almost $850,000. Another example is a teaching hospital, which replaced paper medical charts with electronic medical records (EMR) for outpatients, realizing about $8.6 million in annual savings.[3] This hospital also established electronic access to laboratory results and reports, replacing its manual process for handling medical records and saving $2.8 million a year. Health care organizations also told us that EMRs improved the delivery of care because, among other reasons, more complete medical documentation was available to support the provider's diagnosis. In addition, these electronic records could greatly facilitate the reporting of public health information associated with the early detection and response to disease outbreaks. Additionally, the lessons learned that were reported to us by health care organizations that have successfully implemented solutions could be used by other organizations to accelerate the adoption of health IT. These lessons recognize the importance of reengineering business processes, gaining users' acceptance of IT, providing adequate training, and making systems secure.

Also last year, we reported that multiple federal agencies had a large number of both existing and planned information systems that are intended to support our nation's preparedness for and ability to

---

[3]For electronic medical records (EMRs)—also known as electronic health records, automated medical records, and computer-based patient records, among other names—multiple definitions exist, depending on the functions that are included. They can be used simply as a passive tool to store patient information or can include multiple decision support functions, such as individualized patient reminders and prescribing alerts.

respond to public health emergencies, including bioterrorism.[4] Specifically, these agencies identified 72 systems—34 surveillance systems, 18 supporting technologies, 10 communications systems, and 10 detection systems.[5] For example, the Centers for Disease Control and Prevention is currently implementing its Public Health Information Network, which consists of a number of disease surveillance and communication systems, including the Health Alert Network. This network is an early warning and response system that is intended to facilitate better communication among federal, state, and local agencies during public health emergencies. We also reported that identification and implementation of health care data, communications, and security standards—which are necessary to support compatibility and interoperability of agencies' various IT systems—remained incomplete across the health care sector. A major consequence of not implementing such standards is that federal agencies and others associated with public health cannot exchange data. For example, in responding to the anthrax events, one of the major IT challenges that public health officials faced was the issue of how to exchange data among all participants. During this event, participants accumulated dissimilar data and principally exchanged it manually.

To address the challenges of coordinating the many IT initiatives and implementing a consistent set of standards, we recommended last year that the Secretary of Health and Human Services develop a strategy for public health preparedness and response, to include setting priorities for IT initiatives, establishing milestones for defining and implementing all standards, and establishing mechanisms to monitor the implementation of standards throughout

---

[4]Bioterrorism is the threat or intentional release of biological agents (viruses, bacteria, or their toxins) for the purpose of influencing the conduct of government, or intimidating or coercing a civilian population.

[5]*Surveillance* systems facilitate the performance of ongoing collection, analysis, and interpretation of disease-related data. *Supporting technologies* are tools or systems that provide information for the other categories of systems. *Communications* systems facilitate the secure and timely delivery of information to the relevant responders and decision makers. *Detection* systems consist of devices for the collection and identification of potential biological agents from environmental samples that include an IT component that facilitates the collection of data for surveillance.

the health care industry. Since then, progress has been made in identifying standards. For example, the Office of Management and Budget's Consolidated Health Informatics (CHI) e-government initiative has identified a number of standards that are to be applied to new federal development efforts and modifications of existing systems to promote the interoperability of information across federal agencies. However, implementing these standards across the federal government remains a work in progress. Further progress in leadership has occurred with the President's recently issued Executive Order[6], which calls for the establishment of a National Health Information Technology Coordinator and the issuance of a broader strategic plan to guide the nationwide implementation of interoperable health care information systems. Although it is encouraging that the Coordinator plans to present this strategic plan next week, as health IT initiatives are pursued it will be essential to have continued leadership, clear direction, measurable goals, and mechanisms to monitor progress.

Background

The United States health care system is a large sector of the economy comprised of clinicians, health care delivery organizations, insurers, consumers, and government health agencies. According to the Medicare Payment Advisory Commission, the health care industry generally uses less IT than other industries, and the extent and types of IT deployed vary by setting and institution. The health care industry has recognized that IT can improve the quality of care, promote patient safety, reduce costs of both care and administrative functions, and expedite response to public health emergencies.

Public health officials are increasingly concerned about our exposure and susceptibility to infectious disease and food-borne illness because of global travel, increased volume of food imports,

---

[6]Executive Order 13335—Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator, April 27, 2004.

and the evolution of antibiotic-resistant pathogens. Public health experts maintain that a strong infrastructure could provide the capacity to prepare for and respond to both acute and chronic threats to the nation's health, whether they are bioterrorism attacks, emerging infections, disparities in health status, or increases in chronic disease and injury rates.

IT can play an essential role in supporting federal, state, local, and tribal governments in public health activities and clinical care delivery. For public health emergencies in particular, the ability to quickly exchange data from provider to public health agency—or from provider to provider—is crucial in detecting and responding to naturally occurring or intentional disease outbreaks. It allows physicians to share individually identifiable information with public health agencies for use in performing public health activities.

The Centers for Disease Control and Prevention (CDC) has previously acknowledged several IT limitations in the public health infrastructure. For example, basic capability for disease surveillance systems to detect and analyze disease outbreaks is lacking for several reasons. First, health care providers have traditionally used paper- or telephone-based systems to report disease outbreaks to approximately 3,000 public health agencies. This is a labor-intensive, burdensome process for local health care providers and public health officials, often resulting in incomplete and untimely data. Second, not all public health agencies have access to the Internet or to secure channels for electronically transmitting sensitive data.

Several types of systems can play vital roles in identifying and responding to public health emergencies, including acts of bioterrorism. These types of systems—described in a technology assessment for the Department of Health and Human Services (HHS) that was completed by the University of California San Francisco-Stanford Evidence-based Practice Center—serve different but related functions and include the following:[7]

---

[7]University of California San Francisco-Stanford Evidence-based Practice Center, *Bioterrorism Preparedness and Response: Use of Information Technologies and Decision Support Systems* (Stanford, CA: June 2002).

- **Detection**—systems that consist of devices for the collection and identification of potential biological agents from environmental samples, making use of IT to record and send data to a network.

- **Surveillance**—systems that facilitate the performance of ongoing collection, analysis, and interpretation of disease-related data to plan, implement, and evaluate public health actions.

- **Diagnostic and clinical management**—systems with potential utility for enhancing the likelihood that clinicians will consider the possibility of bioterrorism-related illness. These systems are generally designed to assist clinicians in developing a differential diagnosis for a patient who has an unusual clinical presentation.

- **Communications**—systems that facilitate the secure and timely delivery of information to the relevant responders and decision makers so that appropriate action can be taken.

In April of this year, the President issued an Executive Order, which recognizes the importance of IT to the improvement of the health care system to address problems with high costs, medical errors, and administrative inefficiencies. The order establishes the position of a National Health Information Technology Coordinator. This new position has been tasked with providing leadership for the development and nationwide implementation of interoperable health IT in both the public and private health care sectors. The President also announced a goal of having EMRs available for most Americans within the next 10 years.

Information Technology Can Provide Benefits for Delivery of Care

IT can provide significant benefits in providing clinical health care and in the administrative functions associated with health care delivery. Last October, we identified 20 examples of reported cost savings or other benefits at 14 health care organizations that had implemented IT solutions in their clinical care environments. The

rapidly rising costs of health care, along with an increasing concern for the quality of care and the safety of patients, are driving health care organizations to use IT to automate clinical care operations and their associated administrative functions. IT is now being used for, among other things, EMRs, order management, Internet access for patient and provider communications, and automated billing and financial management.

Health care delivery organizations identified instances that resulted in cost savings from the use of IT as a result of reductions in costs associated with medication errors, communication and documentation of clinical care and test results, staffing and paper storage, and processing of information. Specific examples included:

- A teaching hospital reported that it realized about $8.6 million in annual savings by replacing paper medical charts with EMRs for outpatients. It also reported saving over $2.8 million annually by replacing its manual process for handling medical records with electronic access to laboratory results and reports.

- A teaching hospital reported that it saved $5 million annually on drug substitutions, based on automated prompts that recommended alternatives resulting in increased quality and decreased cost.

- A community hospital prevented the administration of over 1,200 wrong drugs or dosages and almost 2,000 early or extra doses by using bar code technology and wireless scanners to verify both the identities of patients and their correct medications. The reported monetary value of the errors prevented was almost $850,000.

- An integrated health care delivery organization reduced the overall number of daily chart pulls, estimating that about $5.7 million in medical record staffing costs were avoided or saved annually.

IT also contributed to other benefits, such as shorter hospital stays, faster communication of test results, improved management of chronic disease, and improved accuracy in capturing charges associated with diagnostic and procedure codes. For example,

- A teaching hospital reported a decrease in average length of stay from 7.3 to 5 days when it implemented an integrated EMR system that resulted in improvements in health care efficiency and practice changes.

- A teaching hospital reported improved patient scheduling using a rules-based electronic scheduling system that accommodated travel time to the appointment, fasting requirements, and providers' availability.

- An integrated health care delivery organization reported improvements in diabetes control for members with the disease, decreases in upper gastrointestinal studies ordered, and increases in the number of Pap smears performed by using alerts and reminders, automated patient care guidelines, and data warehouse reports.

- A teaching hospital reported that 4 percent of radiology orders that had been entered into the order entry system were cancelled and 55 percent were changed when an embedded alert warned that an order was inappropriate for specified clinical reasons.

Health care organizations also told us that EMRs could also improve the delivery of care because, among other reasons, more complete medical documentation was available to support the provider's diagnosis. In addition, EMRs greatly facilitate the reporting of public health information associated with the early detection of and response to disease outbreaks.

The lessons learned that were reported to us by health care organizations that have successfully implemented IT may prove useful for other organizations as they implement solutions—such as recognizing the importance of reengineering business processes, gaining users' acceptance, providing adequate training, and making systems available and secure. For example, organizations reported that business process changes were key in effectively implementing the technology and that users, including physicians, should be involved in systems design and implementation.

Many IT Initiatives Address the Public Health Infrastructure, Although Standards Implementation Challenges Remain

In May 2003, we reported that six federal agencies involved in bioterrorism preparedness and response had a large number of existing and planned information systems associated with supporting a public health emergency. Specifically, these agencies identified 72 information systems and supporting technologies. Of the 72 systems, 34 are surveillance systems, 18 are supporting technologies, 10 are communications systems, and 10 are detection systems. In spite of these many initiatives, the key ones that are intended to facilitate greater information sharing are still being developed and implemented. For example, CDC is currently implementing its Public Health Information Network, which consists of a number of disease surveillance and communications systems, including the Health Alert Network. This network is an early warning and response system intended to provide federal, state, and local agencies with better communications during public health emergencies. The Department of Defense is using its Electronic Surveillance System for the Early Notification of Community-based Epidemics (ESSENSE) to support early identification of infectious disease outbreaks in the military by comparing analyses of data collected daily with historical trends. We also found that agencies varied in the extent to which they interacted and coordinated with other agencies in planning and operating each of these initiatives.

The October 2001 anthrax attacks and the subsequent emergence of new infectious diseases have highlighted the importance of data standards for real-time data exchange across the public health infrastructure. During the anthrax attack, participants accumulated dissimilar data and principally exchanged it manually.

Since 1993, we have called for federal leadership to expedite the standards development process in order to accelerate the use of EMRs.[8] Most recently, in May 2003, we again reported that the

---

[8]U.S. General Accounting Office, *Automated Medical Records: Leadership Needed to Expedite Standards Development*, GAO/IMTEC-93-17 (Washington, D.C.: April 30, 1993).

identification and implementation of health care data, communications, and security standards—which are necessary to support the compatibility and interoperability of agencies' various IT systems—remains incomplete across the health care industry. We also identified other standards setting initiatives (e.g., CHI and HIPPA[9]) and raised concerns about coordinating these initiatives.

To address the challenges of coordinating the many IT initiatives and implementing a consistent set of standards, we recommended that the Secretary of Health and Human Services (HHS), in coordination with other key stakeholders, establish a national IT strategy for public health preparedness and response, including specific steps toward improving the nation's ability to use IT in support of the public health infrastructure. Specifically, we recommended, among other things, that the Secretary

- set priorities for information systems, supporting technologies, and other IT initiatives;

- 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 all standards; and

- create a mechanism—consistent with HIPAA requirements—to monitor the implementation of standards throughout the health care industry.

Since our May 2003 report, HHS has continued its efforts to identify applicable standards throughout the health care industry and across federal health care programs. For example, in May 2004, the CHI

---

[9]In August 1996, Congress recognized the need for standards to improve the Medicare and Medicaid programs in particular and the efficiency and effectiveness of the health care system in general. It passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which calls for the industry to control the distribution and exchange of health care data and begin to adopt electronic data exchange standards to uniformly and securely exchange patient information.

initiative—one of OMB's e-government projects—announced fifteen additional standards that build on the initial five announced in March 2003. Federal agencies are expected to include the standards in their architectures and when they build, acquire, or modify systems. Current plans for the CHI initiative call for it to be incorporated into HHS's Federal Health Architecture by September 2004.[10] This architecture is still evolving, and many issues—such as coordination of the various standards setting efforts and implementation of the standards that have been identified—are still works in progress. Until these standards are more fully implemented, federal agencies and others associated with the public health infrastructure cannot ensure that their systems will be capable of exchanging data with other systems when needed and consequently cannot ensure effective preparation for and response to public health emergencies, including acts of bioterrorism.

In addition, in April of this year, the President issued an Executive Order, which calls for the establishment of a National Health Information Technology Coordinator and the issuance of a broader strategic plan to guide the nationwide implementation of interoperable health care information systems. The coordinator is also specifically tasked with creating incentives for the use of health IT and accelerating the adoption of EMRs, among other things. The Coordinator plans to present the strategic plan next week. Such a plan, if properly crafted, should help to move the health care industry towards interoperable information systems. As health IT initiatives are pursued, it will be essential to have continued leadership, clear direction, measurable goals, and mechanisms to monitor progress.

In summary, there are many opportunities and challenges associated with the implementation of IT for clinical care delivery and public health. The federal government, namely HHS, has taken a leadership role in establishing a strategy and identifying data and

---

[10]Initiated in July 2003, the Federal Health Architecture is expected to define an overarching framework and methodology for establishing targets and standards for interoperability and communication across the federal health community.

communications standards, which are critical for sharing data across the health care industry—both to improve the quality of patient care in the United States and to strengthen the public health infrastructure. However, much more work remains to more fully utilize IT for the delivery of care and to identify and respond to public health emergencies. HHS needs to provide continued leadership, sustained and focused attention, clear direction, and mechanisms to monitor progress in order to bring about measurable improvements and achieve the President's goals.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions that you or members of the subcommittee may have at this time.

If you should have any questions about this testimony, please contact me at (202) 512-9286 or M. Yvonne Sanchez, Assistant Director, at (202) 512-6274. We can also be reached by e-mail at pownerd@gao.gov and sanchezm@gao.gov, respectively. Other individuals who made key contributions to this testimony include Joanne Fiorino, M. Saad Khan, and Mary Beth McClanahan.

GAO's Mission	The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."
Order by Mail or Phone	The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to: U.S. Government Accountability Office 441 G Street NW, Room LM Washington, D.C. 20548 To order by Phone: Voice: (202) 512-6000 TDD: (202) 512-2537 Fax: (202) 512-6061
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Web site: www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400 U.S. Government Accountability Office, 441 G Street NW, Room 7125 Washington, D.C. 20548
Public Affairs	Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, D.C. 20548