United States Government Accountability Office

GAO

Report to Congressional Committees

February 2010

ELECTRONIC PERSONAL HEALTH INFORMATION EXCHANGE

Health Care Entities' Reported Disclosure Practices and Effects on Quality of Care

GAO

Accountability * Integrity * Reliability

GAO-10-361

G A O
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-10-361, a report to congressional committees

February 2010

ELECTRONIC PERSONAL HEALTH INFORMATION EXCHANGE

Health Care Entities' Reported Disclosure Practices and Effects on Quality of Care

Why GAO Did This Study

To promote the use of information technology for the electronic exchange of personal health information among providers and other health care entities, Congress passed the Health Information Technology for Economic and Clinical Health (HITECH) Act. It provides incentives intended to promote the widespread adoption of technology that supports the electronic sharing of data among hospitals, physicians, and other health care entities. Pursuant to a requirement in the HITECH Act, GAO is reporting on practices implemented by health information exchange organizations, providers, and other health care entities that disclose electronic personal health information.

GAO's specific objectives were to describe (1) the practices implemented for disclosing personal health information for purposes of treatment, including the use of electronic means for obtaining consent, as reported by selected health information exchange organizations, their participating providers, and other entities; and (2) the effects of the electronic sharing of health information on the quality of care for patients as reported by these organizations.

To address both objectives, GAO conducted case studies of 4 of more than 60 operational health information exchanges and a selection of each of the exchanges' participating providers.

View GAO-10-361 or key components.
For more information, contact Valerie C. Melvin at (202) 512-6304, Linda T. Kohn at (202) 512-7114, or Gregory C. Wilshusen at (202) 512-6244.

What GAO Found

The health care entities GAO studied reported that they implement disclosure practices that reflect widely accepted practices for safeguarding personal information–the Fair Information Practices–to help ensure the appropriate use and disclosure of electronic personal health information for treatment purposes. For example, providers in the study described various implementations of practices that require direct interaction with patients, such as informing patients of the use and disclosure of personal health information and providing patients access to their own records. Some of them inform patients that their electronic personal health information may be shared through health information exchanges–entities that were formed to facilitate the electronic sharing of patients' health information among providers. Both the providers and exchanges in the study described practices that limit disclosure of information, secure electronic information that they store and transmit, and help ensure accountability for safeguarding electronic personal health information.

Although the health information exchanges reported that they have not conducted formal studies or evaluations of the overall effect of electronically sharing personal health information, both the exchanges and providers reported examples of ways that sharing electronic personal health information about patients has had a positive effect on the quality of care that providers deliver to patients.

- Officials from two exchanges stated that they provide a direct connection from participating hospitals to their state's Department of Public Health for real-time reporting of conditions and for supporting the early detection of disease outbreaks. According to one of these officials, this service facilitated the state's ability to obtain information about cases of H1N1 more quickly than other states.

- A large hospital that participated in one of the exchanges reported that a cardiologist was able to obtain an abnormal laboratory result electronically from the exchange one day earlier than they would have otherwise. This timely access to the patients' electronic health information allowed the provider to perform earlier intervention for a potentially life-threatening condition.

- Another hospital reported that information obtained through its health information exchange helped its emergency department physician ascertain that a patient who was requesting medication for pain had been in five area hospitals in seven nights seeking pain medication. As a result, the physician did not prescribe any additional pain medication.

Contents

Tables

Figure

Abbreviations

HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health
OECD	Organization for Economic Cooperation and Development

GAO

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

February 17, 2010

Congressional Committees

Studies published by the Institute of Medicine and other organizations have shown that the fragmented and inaccessible state of medical information can adversely affect the quality of health care and compromise patient safety.[1] This is important because patients may visit a variety of different health care providers to meet their health care needs. For example, for treatment of a chronic condition, a patient could visit a primary care doctor, a specialist, a clinical laboratory, an imaging center, and a pharmacy. Each of these providers may maintain records of medical treatment, laboratory results, medications, and health history and personal information about the patient that may also be needed by other providers but is not readily available except in printed form. As a result, providers may not have access to critical information needed to treat patients, such as allergies to medicines, timely lab test results, and medical histories.

The use of information technology to electronically collect, store, and share patients' personal health information[2] could help providers obtain information about patients more quickly than they can in the current medical records environment.[3] Over the past several years, an increasing number of organizations have implemented technology to enable the electronic exchange of personal health information among providers, including health information exchanges (HIE). These exchanges provide the technology and facilities needed to support the electronic sharing of data among hospitals, physicians, clinical laboratories, radiology centers, pharmacies, health plans (insurers), and public health departments. Other

[1] Institute of Medicine, *Crossing the Quality Chasm: A New Health System for the 21st Century* (Washington, D.C.: Mar. 1, 2001); "Missing Clinical Information During Primary Care Visits," Peter C. Smith, et. al.; Journal of the American Medical Association, vol. 293 no. 5: 565-571.

[2] Personal health information is information relating to the health or health care of an individual that can be used to identify the individual. It includes information such as patients' demographic, financial, and clinical information, along with laboratory test results or medical images.

[3] Congressional Budget Office, *Evidence on the Costs and Benefits of Health Information Technology* (Washington, D.C.: May 2008).

types of entities, such as integrated health care delivery systems,[4] have also increased the extent to which they share patients' personal health information electronically among providers.

While sharing health information electronically can help providers obtain more timely and accurate information about the patients they are treating, it may also increase the potential for misuse of personal health information for illegal purposes, such as discriminatory employment practices and health identity theft.[5] Additionally, health information exchanges report challenges in implementing practices that not only enable the effective sharing of data but also ensure the appropriate use and disclosure of personal health information.[6] These factors may limit the extent to which health care providers participate in electronic sharing of their patients' health information.[7]

However, providers and patients have reported some benefits resulting from the electronic sharing of health information, such as increased patient safety, improved quality of health care, enhanced efficiency of administrative functions, and reduced costs.[8] Additionally, in a 2008 report the Congressional Budget Office[9] described benefits resulting from the electronic sharing of personal health information, including decreases in the duplication of diagnostic procedures and prevention of medical errors.

[4] An integrated health care delivery system is a network of organizations that provides or arranges to provide a coordinated continuum of services to a defined population and is willing to be held clinically and fiscally accountable for the outcomes and health status of the population served.

[5] Markle Foundation, *Connecting for Health Common Framework: The Architecture for Privacy in a Networked Health Information Environment* (New York, N.Y.: April 2006).

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

[7] GAO-07-238.

[8] eHealth Initiative, *Migrating Toward Meaningful Use: The State of Health Information Exchange* (Washington, D.C.: August 2009). GAO, *Information Technology: Benefits Realized for Selected Health Care Functions*, GAO-04-224 (Washington, D.C.: October 2003).

[9] Congressional Budget Office, *Evidence on the Costs and Benefits of Health Information Technology* (Washington, D.C.: May 2008).

To promote the use of information technology for the electronic exchange of personal health information among providers and other health care entities, Congress passed the Health Information Technology for Economic and Clinical Health (HITECH) Act as part of the American Recovery and Reinvestment Act of 2009,[10] which the President signed into law on February 17, 2009.[11] HITECH provides financial incentives, in the form of grants and Medicare reimbursements, to promote the widespread adoption of technology that supports the electronic sharing of personal health information among health care entities, such as hospitals, physicians, clinical laboratories, and public health agencies. In response to the need to better define practices for ensuring that this information is appropriately disclosed to authorized entities, the HITECH Act extends existing federal privacy and security requirements to certain organizations, such as health information exchanges, that facilitate the sharing of electronic personal health information.

The HITECH Act requires us to report on practices implemented by health information exchange organizations, providers, and other health care entities for disclosing electronic personal health information. As agreed with committee staff, our specific objectives were to describe the practices implemented for disclosing personal health information for purposes of treatment, including the use of electronic means for obtaining consent, as reported by selected health information exchange organizations, their participating providers, and other entities and the effects of the electronic sharing of health information on the quality of care for patients as reported by these organizations.

To address both objectives, we conducted case studies of 4 of more than 60 health information exchange organizations that were reported to be operational. We also studied a selection of each of the exchanges' participating providers that share information with other providers through the exchange and directly with other providers (that are not members of the exchange). These providers were identified by the exchanges as active users of the HIEs' services. In conducting the case studies, we identified ways the exchanges and their participating providers addressed selected disclosure practices, but we did not assess the implementation of these practices. We also used the case studies to obtain

[10] Pub. L. No.: 111-5, div. A, title XIII, 123 Stat. 115, 226 (Feb. 17, 2009).

[11] Pub. L. No. 111-5, 123 Stat. 115 (Feb. 17, 2009).

information on the effect that the electronic sharing of health information had on the quality of care.

To supplement the information we collected through the case studies, we gathered information from and conducted interviews with other health care entities (two integrated health care delivery systems), two professional associations (eHealth Initiative and Healthcare Information Management and Systems Society), and one state's electronic health collaborative, an organization focused on developing and enforcing statewide health information sharing policy. The information we obtained through the case studies and from other entities about both disclosure practices and quality of care cannot be generalized.

We conducted our work from May 2009 to February 2010 in accordance with all sections of GAO's Quality Assurance Framework that are relevant to our objectives. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations in our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any findings and conclusions.

Appendix I contains further details about our scope and methodology, including the methodology and criteria we applied in selecting health information exchanges for our case studies.

Background

According to recent studies on the adoption of health information technology,[12] most health care providers in the United States still use paper health records to store, maintain, and share patients' information. Sharing this information among multiple providers treating the same patient requires transferring paper documents by mail, fax, or hand delivery. In addition to being slow and cumbersome, these methods of transferring health information can result in loss or late delivery of the information, which may require the requesting provider to conduct

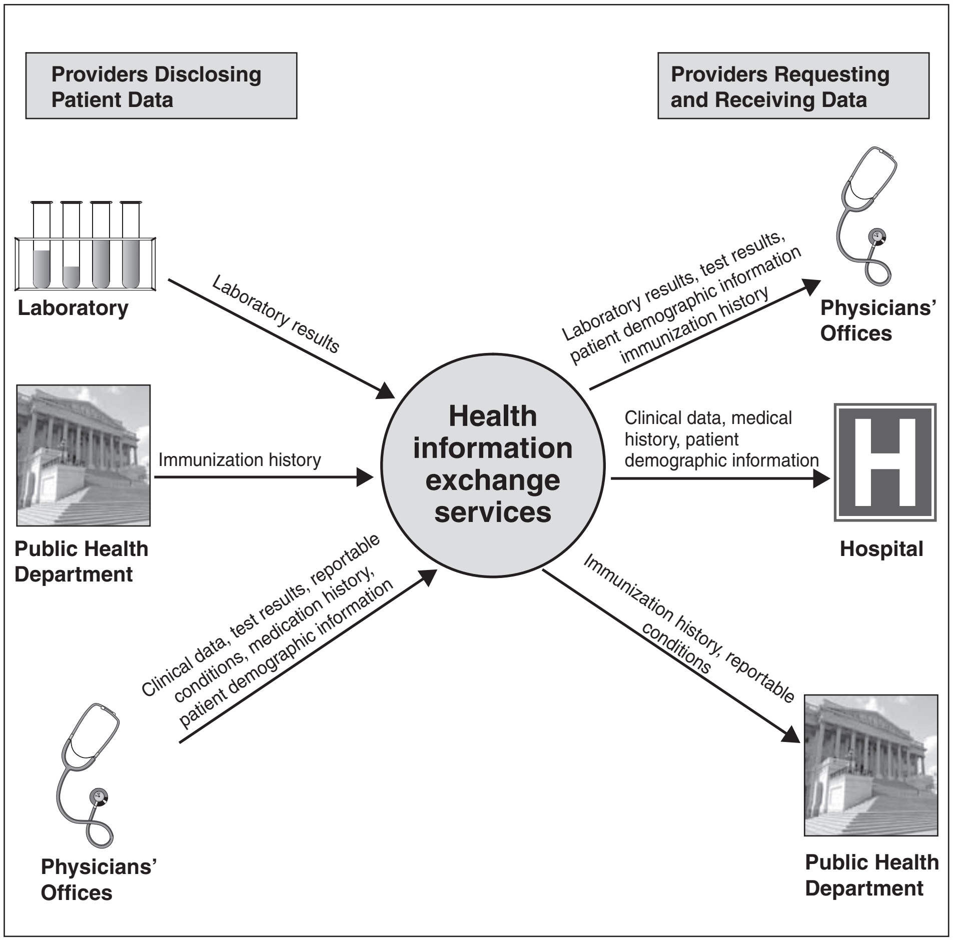
[12] See *Health Information Technology in the United States: The Information Base for Progress*, Robert Wood Johnson Foundation, et. al., (Princeton, N.J.: Oct. 10, 2006); *Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records*, NET Institute Working Paper No. 07-16, Miller, Amalia R. and Tucker, Catherine (Department of Economics, University of Virginia, Charlottesville, Va.; Sloan School of Management, Massachusetts Institute of Technology, Cambridge, Ma: February 2009); "The Use of Electronic Health Records in U.S. *Hospitals,"* AK Jha et. al., *The New England Journal of Medicine*, vol. 360, no. 16, pp. 1628-1638 (Boston, Ma., Apr. 16, 2009).

duplicate tests, or may contribute to medical errors due to the lack of information needed to properly treat the patient. Additionally, the physical delivery of paper health records typically does not provide an effective means for securing the information while it is being transferred, nor does it provide ways to identify who accesses the records or discloses the information contained in the records.

In part to address these types of deficiencies, health care providers have been adopting electronic health information systems to record, store, and maintain patients' information. As more providers have adopted and used these systems, additional capabilities have been developed and implemented, including the ability to electronically share patients' information from a provider directly to other providers, or among providers participating in an HIE.

HIEs facilitate the sharing of electronic health information by providing the services and technology that allow providers (such as physicians, hospitals, laboratories, and public health departments) to request and receive information about patients from other providers' records. For example, when a provider requests information through the exchange, the HIE identifies the source of the requested data, then initiates the electronic transmission that delivers the data from the provider that is disclosing the patient's information to the provider that requested the information. A simplified model of this exchange activity is shown in figure 1.

Figure 1: Simplified Model of Electronic Health Information Exchange


Providers Disclosing Patient Data
Providers Requesting and Receiving Data
Laboratory
Laboratory results
Public Health Department
Immunization history
Clinical data, test results, reportable conditions, medication history, patient demographic information
Physicians' Offices
Health information exchange services
Laboratory results, test results, patient demographic information immunization history
Physicians' Offices
Clinical data, medical history, patient demographic information
H
Hospital
Immunization history, reportable conditions
Public Health Department

Sources: GAO analysis of HIE data and Art Explosion (clip art).

Research indicates that most HIEs were formed to share information among health care providers and organizations within a geographic area (e.g., metropolitan area, state, region, or nation). However, others were designed for unique purposes, such as to collect and share information about participants involved in a state Medicaid program or to aggregate information about patients within a community, state, or region in support of efforts to improve the health of a population.

The ways that HIEs are established and managed vary. Some are established by state governments, while others are established by private organizations. They may be managed by public-private partnerships or other organizations that were created to promote collaboration among health care providers.

Efforts in the United States to establish organizations that facilitate the sharing of electronic health information among providers began in the early 1990's. These organizations, called Community Health Information Networks, evolved into Regional Health Information Organizations throughout the early to mid 2000s. Since then, there has been a steady increase in the number of HIEs that are fully operational and actively facilitate the electronic sharing of patients' health information. In 2007, the eHealth Initiative reported that, in a nationwide survey, it had identified 32 operational HIEs.[13] One year later, its survey identified 42 operational exchanges, representing a 31 percent increase.[14] Then, in 2009, the survey identified 57 operational exchanges, a nearly 36 percent increase from 2008.[15]

Most of the nearly 150 exchanges that responded to the eHealth Initiative's 2009 survey reported that they were not yet engaged in the electronic exchange of health information but were involved in activities such as defining a business plan, identifying participants' information requirements, and securing funding. Others responded that they were in the process of defining and implementing technical, financial, and legal procedures. The 57 operational HIEs that responded to the survey reported that they support a variety of information-sharing services for their participating providers. The most common services included the delivery of laboratory and test results and clinical documentation, electronic health records, electronic prescribing, and alerts about critical conditions, such as adverse drug interactions. Other services included data sharing for public health purposes, such as for tracking and managing

[13] eHealth Initiative, *eHealth Initiative's Fourth Annual Survey of Health Information Exchange At the State and Local Levels: Overview of 2007 Findings* (Washington, D.C.: December 2007).

[14] eHealth Initiative, *eHealth Initiative's Fifth Annual Survey of Health Information Exchange* At *the State and Local Levels* (Washington, D.C.: September 2008). The eHealth Initiative also reported in 2008 that all 32 operational exchanges that responded to the 2007 survey continued to be in operation.

[15] eHealth Initiative, *Migrating Toward Meaningful Use: The State of Health Informaiton Exchange* (Washington, D.C.: August 2009). Of the 193 HIEs surveyed, 150 responded to the annual survey of health information exchange organizations.

childhood immunizations, and for reporting health care quality measures to participating providers.[16]

Widely Accepted Privacy Practices Provide a Framework for Protecting Electronic Personal Health Information

The United States and several other countries base privacy laws and policies on practices for protecting personal information, including health information. While there is no single federal law in the United States that defines requirements for protecting electronic personal health information from inappropriate use or disclosure, there are a number of separate laws and policies that provide privacy and security protections for information used for specific purposes or maintained by specific entities. Further, some states impose additional restrictions on the use and disclosure of personal health information through state laws and regulations, while others do not define restrictions beyond those imposed by federal rules.

Fair Information Practices

Privacy experts refer to a set of basic principles, known as Fair Information Practices, as a framework for protecting personally identifiable information such as personal health information. These practices were first proposed in 1973 by a U.S. government advisory committee.[17] The practices provided the basis for subsequent laws and policies in the United States and other countries.[18] While there are different versions of Fair Information Practices, their core elements are reflected in the privacy and security regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[19] and in the seven key practices that we addressed with the case study HIEs and providers. They are described in table 1.

[16] The Medicare Prescription Drug, Improvement, and Modernization Act of 2003 created a financial incentive for hospitals to submit to the Centers for Medicare & Medicaid Services data that are used to calculate hospital performance on measures of the quality of care provided. See Pub. L. No. 108-173, § 501(b), 117 Stat. 2066, 2289-90.

[17] U.S. Department of Health, Education, and Welfare, *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (Washington, D.C.: July 1973).

[18] The Privacy Act of 1974 (5 U.S.C. § 552a); The Organization for Economic Cooperation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris, France: Sept. 23, 1980); U.S. Department of Homeland Security, Privacy Policy Guidance Memorandum 2008-01, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (Dec. 29, 2008).

[19] HIPAA was enacted into law as Pub. L. No. 104-191, Title II, Subtitle F, 110 Stat. 1936, 2021 (codified at 42 U.S.C. §§ 1320d–1320d-8). The HIPAA Privacy and Security Rules were promulgated at 45 C.F.R. Parts 160 and 164. HIPAA, Pub. L. No. 104-191, title II, subtitle F (Aug. 21, 1996).

Table 1: Seven Widely Accepted Fair Information Practices for Protecting Personally Identifiable Information

Practices	Description
1. Informing individuals about the use of their information and how it is to be protected	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
2. Obtaining individual consent	The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
3. Facilitating individual access to and correction of records	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
4. Limiting use and disclosure to a specific purpose	Personal information should not be disclosed or otherwise used for other than a specified purpose without the consent of the individual or legal authority. The purposes for the collection of personal information should be disclosed before collection and upon any change to that purpose, and its use should be limited to those purposes and compatible purposes.
5. Providing security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
6. Ensuring that data are accurate, timely, and complete	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
7. Establishing accountability for how personal information is protected	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

Source: GAO analysis of Fair Information Practices.

Health Insurance Portability and Accountability Act of 1996

The HIPAA Privacy and Security Rules define the circumstances under which personal health information may be disclosed by covered entities[20] to other entities, such as providers, patients, health plans (insurers), and public health authorities. The HIPAA Privacy Rule places certain limitations on when and how covered entities may use and disclose personal health information. However, the Privacy Rule permits the use or

[20] Covered entities are defined under regulations implementing HIPAA as health plans that provide or pay for the medical care of individuals, health care providers that electronically transmit health information in connection with any of the specific transactions regulated by the statute, and health care clearinghouses that receive health information from other entities and process or facilitate the processing of that information into standard or nonstandard format for those entities. 45 C.F.R. § 160.103. HIEs are typically considered to be business associates of their participating providers which, as covered entities, are required to obtain through formal agreement satisfactory assurance that their business associates will appropriately safeguard protected health information. However, the HITECH Act has expanded the responsibility of business associates for certain privacy and security requirements and extended penalties for noncompliance.

disclosure of personal health information for treatment, payment, and other health care operations. To ensure that this information is reasonably protected from unauthorized access, the HIPAA Security Rule[21] specifies a series of administrative, technical, and physical security practices for providers and plans to implement to ensure the confidentiality of electronic health information.

Health Information Technology for Economic and Clinical Health Act

The HITECH Act includes a series of privacy and security provisions that expand certain provisions under HIPAA. Although final regulations for implementing these provisions remain under development, HITECH requires certain entities that were not initially covered by HIPAA, which may include health information exchanges, to meet the requirements defined in the HIPAA privacy and security rules. Further, if certain conditions are met, the act may limit the disclosure of information to health plans (insurers) upon patient request. HITECH also provides an individual with a right to receive an accounting of disclosures of patient information (for the purposes of treatment, payment, and health care operations) from covered entities using electronic health records.

HIEs and Providers Describe Various Methods of Implementing Disclosure Practices

The four exchanges in our case studies reported that they implement various practices to ensure appropriate disclosure of electronic personal health information for treatment purposes. The 18 case study providers that participate in these exchanges also described practices they implement for disclosing patients' personal health information when the information was shared through an HIE or directly with other providers. Some of the providers reported that they inform patients that their electronic personal health information may be shared through a health information exchange. The practices reported by the HIEs and providers reflect the seven Fair Information Practices that we described. In all cases, the providers we studied stated that their participation in an HIE did not require them to change their established practices for disclosing and safeguarding patients' personal health information.

While providers take responsibility for implementing the three practices that involve direct contact with patients (providing information about and obtaining consent for use and disclosure, and making corrections to personal health information), both providers and exchanges share responsibility for implementing the other four practices. For example, the

[21] 45 C.F.R. §§ 164.302-164.318.

18 case study providers inform their patients about the use of personal health information by giving notices of privacy practices and by other means. They also obtain patients' consent to disclose health information for purposes of treatment, payment, and operation. Additionally, providers stated that they implement practices to facilitate patients' ability to access and request corrections to personal health information, and all the HIEs and providers described practices intended to limit the disclosure and use of information to specific purposes. They also described practices they implement that are intended to address security, data quality, and accountability for protecting electronic personal health information. Detailed information about the privacy practices identified by our case study organizations is included in appendix II.[22]

Providers Reported That They Inform Patients about the Use of Their Information and How It Is to Be Protected, but Most Do Not Inform Patients about Sharing through an HIE

All of the 18 providers in our case studies inform their patients of their overall privacy practices by giving them a notice in paper form, and 13 of them post a copy of the notice on their Web site. These notices state that the provider intends to use and disclose patients' personal health information for treatment purposes, explain the provider's commitment to protect that information and how it intends to do so, and inform patients about their right to take action if they believe their privacy has been violated.

Six of the case study providers stated that they inform patients by various methods that personal health information will be shared with other providers through an HIE. Three of the six providers include this information in the paper privacy notices that they give to patients, and three providers use other methods to inform patients of their participation in an HIE. For example, two providers inform patients by displaying materials, such as posters, in the waiting room.[23] Another informs patients that their information will be shared electronically when obtaining consent to disclose information for treatment purposes.

[22] The other entities with whom we spoke described practices similar to those described by our case study HIEs and providers.

[23] Although HIEs are not directly involved in providing notices of privacy practices to patients, some of our case study HIEs described activities intended to support providers' efforts to address this element of disclosure. For example, some HIEs stated that they provide materials that may be used to inform and educate patients about electronic information exchange through the HIE.

Providers Reported Various Methods of Obtaining Patients' Consent for Sharing Personal Health Information, but None Has Implemented Electronic Consent

As with giving notice, all case study providers that treat patients stated that they obtain and document patients' consent for disclosure, most often doing so by having patients sign paper forms that include language authorizing the disclosure of personal health information for treatment, payment, and health care operations.[24] However, the 15 providers that send patients' information to other providers through an HIE described varying approaches for obtaining patients' consent.[25] For example, 14 of the providers rely on patients' general consent; 8 of the 14 do not give patients an option to exclude their health information from the HIE.[26] Six case study providers assume patients are willing to have their information shared through an exchange unless this consent is explicitly denied. The other one of these 15 providers actively seeks patient consent to share information through the exchange before it allows such sharing to take place. The practice of obtaining patients' consent for sharing their information through an HIE is intended to help ensure that patients are aware of how and with whom their information is being shared.

None of the case study providers had implemented electronic means for obtaining patients' consent for disclosure. However, one HIE had developed an electronic tool that its providers use to record patients' consent preferences that are obtained by other means.

[24] Seventeen providers reported that they obtain patients' consent at each visit by providing notice of privacy practices, and one obtains consent at patients' initial visit and again whenever its notice of privacy practices changes.

[25] The other three case study providers obtain patients' information from an HIE but do not yet share their own patients' electronic health information through an exchange.

[26] Most case study providers had determined that the patient's written consent for disclosure of information for treatment, payment, and health care operations was legally sufficient to permit disclosure of health information to the HIEs since those organizations were intended to facilitate the transmission of data among providers for treatment. Those providers did not obtain additional consent specifically for sharing information through the HIEs.

Providers Reported That They Implement Similar Methods to Facilitate Patients' Access to Their Personal Health Information and to Request Corrections

Allowing patients to review their personal health information and request corrections to their records helps ensure that patients have a way to verify the accuracy and integrity of their personal health information. Seventeen of the 18 providers in our case studies reported that they require patients to request access to their information in writing and to then view or obtain their information in person. In most cases, providers require patients to submit a written request for a correction. The correction is included in the patients' records after a doctor determines that it is appropriate. One provider allowed patients to use a Web portal to view the demographic and medical information in their files and to request changes to that information.

Once a correction to a patient's record has been made by a provider, it may be difficult to ensure that the same correction is made in the records of other providers with whom the patients' information has been previously shared through an HIE. While the case study exchanges are not directly involved with patients' requests, two reported that they help providers remain up-to-date with patients' corrected records. For example, these exchanges stated that they generate reports that identify where patient information has been shared. Providers can use this information to notify other providers about corrections and better ensure that the patient's information remains consistent and up-to-date with all providers.

HIEs and Providers Described Similar Practices for Limiting Disclosure with Exceptions for Emergency Situations

The four HIEs and 18 providers also described steps they take to limit the use of personal health information to specific purposes. All of the exchanges and providers reported that they limit disclosures by implementing role-based access controls through their systems.[27] For example, HIEs and providers generally grant individuals involved in treating patients, such as physicians and nurses, access to all patient information, while those whose roles are limited to administrative functions (e.g., scheduling appointments) are provided access only to information relevant to those functions, such as patient demographics.[28] Further, two of the exchanges limit the amount and types of patient information shared with their participating providers to certain types of

[27] Role-based access controls are security measures used to determine the amount and types of information allowed to users based on the functions a user is allowed to perform within an organization.

[28] The various roles and the information they are allowed to access are defined by the provider organizations.

data, such as those specified in standard continuity of care documents[29] or in summary reports defined by the HIEs and their participating providers. Fifteen providers stated that when they receive requests for a patient's information directly from other providers (that do not participate in the HIE), they examine requests on a case-by-case basis. Based on the examinations, these providers limit disclosure to the data they determine is appropriate to address the purpose of each request. By taking these steps, the case study exchanges and providers intend to limit sharing of electronic personal health information to specific purposes and to protect this information from inappropriate use and disclosure.

While HIEs and providers described ways that they limit the disclosure of information in ordinary circumstances, three of the exchanges also reported that they have provisions for allowing special access to electronic information in emergency situations.[30] All the exchanges in our study allow authorized emergency department physicians full access to data for patients they treat. One also allows providers broader access to patient information for some non-emergency situations, such as when obtaining historical information about new patients. In those cases, users are able to access data on any patient by providing a justification for the need to access the information. By allowing access to the electronic information about patients that they have stored in their health information systems, the HIEs support the providers' ability to provide care to new patients and to patients in emergency situations.

HIEs and providers said that they limit disclosure of patient information for uses other than treatment—i.e., secondary uses—to the purposes allowed by the HIPAA Privacy Rule. Specifically, the rule allows reporting de-identified health data to public health agencies for purposes such as disease tracking[31] and sharing health information with medical research

[29] One HIE extracts patient information from some of its providers' electronic health record systems and shares "continuity of care documents" that meet standards defined by a federal standards organization. The standard summary view providers receive when they search HIE systems typically includes laboratory results, patient demographic information, and recent hospital discharge information.

[30] About half of the case study providers reported that they typically do not receive requests from other providers for electronic information for emergency treatment. They address requests in emergency situations through traditional practices such as faxing information to hospitals or providing information via telephone.

[31] De-identified health information does not identify or provide a reasonable basis to identify a patient.

facilities.[32] However, representatives from one case study HIE described an additional secondary use of the personal health information for a quality improvement program that it conducts. This exchange analyzes participating providers' overall performance based on specific indicators (e.g., performing mammograms, screening for diabetes, and providing well checks for children and infants) and compares their performance to that of other providers that treat similar patient populations.[33] By showing providers how they compare to their peers in providing chronic care treatment and preventive care to patients, these reports encourage providers to match their performance with that of their peers.

HIEs and Providers Reported Various Methods of Securing Patients' Personal Health Information against Improper Use and Disclosure

In addition to the steps they take to limit the disclosure of personal health information, HIEs and providers described practices they implement for securing patients' electronic personal health information against misuse and inappropriate disclosure. These practices include mechanisms intended to limit access to health information systems and patients' data that are stored in these systems, and to secure data during transmission.

All the case study HIEs and providers reported that they register and approve users before they are allowed access to their systems (i.e., the HIEs' information systems and the providers' own internal health information systems). They require users to log in to the systems with unique user names and passwords that were established during registration. In addition, two of the exchanges and five providers reported that they take more rigorous steps for verifying users' identities. For example, one exchange implemented a two-stage login process that requires users to identify pictures that they select during registration in addition to confirming the user's name and password. In two cases, providers' systems require the entry of an additional code generated by a

[32] Disclosure of personal health information for research purposes requires prior written authorization from the patient or a waiver from an institutional review board. An institutional review board is a group of scientists, doctors, clergy, and consumers that reviews and approves action plans for clinical research. Every health care facility that conducts clinical research has such a board.

[33] Although other HIEs we studied are considering similar uses of data, one of them prohibits such use.

security token before allowing users to log in from a remote location (i.e., a location other than the place of employment).[34]

HIEs also described additional steps they take to restrict access to patients' personal health information. For example, one requires providers to enter patient identification information when requesting data from other providers' records; this practice is intended to restrict providers' access to data about patients they are treating at the time of the request. Another limits the time period for which a provider can access a patient's information—i.e., providers can only access information for a 90-day treatment period. One of the exchanges described a role-based method it had implemented for restricting access to system data. In this case, the system requires and verifies additional information about the requester before allowing access to certain data stored in the system. By restricting access to the systems in which patient information is stored and to only the information needed by providers for treating a patient, HIEs intend to protect the personal health information that they maintain in their systems from access by unauthorized individuals.

In addition to access control mechanisms, HIEs and their participating providers reported that they implement a combination of practices to ensure that the data they store are secure. The HIEs in our case studies reported that they intend to store all electronic patient data indefinitely to accommodate legal requirements and varying data retention requirements.[35] Most HIEs stated that they store detailed personal health information on patients, although the types and amount of stored data varies. For example, two of the exchanges store all patient health information that is sent from participating providers. Representatives of two other exchanges reported that they do not provide a repository for personal health information but retain limited information, such as (1) demographic information used to identify the patient, including the patient's name and date of birth; (2) identifying information used to locate

[34] Security tokens are portable devices, such as a smart card or a device that displays time-synchronized identification codes, which are used to establish the identity of users.

[35] Accepted privacy principles generally call for the destruction of data after a specified time period in order to reduce the likelihood that the data will be improperly accessed, lost, or misused, patient data are subject to regulations intended to ensure that it remain available as long as may be necessary for treatment purposes. Additionally, state requirements for retaining different types of records, such as digital images and those related to mental health, vary, and some states specify how long certain types of health care organizations such as hospitals and clinical laboratories should retain their data.

patients' records when users search for data; and (3) data for maintaining an audit trail of access and use of patients' personal health information. These HIEs described technical safeguards they implement for protecting the data that they store, such as the use of virtual private networks, firewalls, and intrusion detection systems.[36] Providers reported that they implement similar security mechanisms to protect the electronic personal health information that they store.

Additionally, all the exchanges and ten of the providers reported that they implement practices for securing personal health information that is transmitted electronically to an HIE or other providers. They stated that the data that they share electronically are encrypted prior to the data being transmitted. The implementation of these mechanisms is intended to prevent unauthorized individuals from accessing data being stored or transmitted for misuse, such as exploitation of confidential information for monetary gain or health identity theft.

HIEs and Providers Described Steps They Take to Ensure That Shared Patient Data Are Accurate and Complete

To ensure that the information they share about patients is accurate and complete, the HIEs and providers stated that they conduct testing and other activities to verify the quality of their data. Specifically, all the exchanges stated that they perform data quality testing prior to incorporating providers' data into their systems. This testing entails the use of automated tools to verify that patients and data are matched accurately, along with manual reviews of data performed by personnel within the HIE. However, all of the exchanges generally rely on their participating providers to ensure the accuracy and completeness of patients' personal health information; they stated that their responsibility is limited to maintaining the quality of the data as it is received from and transmitted to providers.

In addition, providers described practices for ensuring the quality of patient data that they maintain in their own health information systems and share through HIEs. For example, 13 of the providers told us that they

[36] A virtual private network is a data network that enables two or more parties to communicate securely across a public network by creating a private connection, or "tunnel," between them. A firewall is a hardware or software component that protects computers or networks from attacks by outside network users by blocking and checking all incoming traffic. An intrusion detection system detects inappropriate, incorrect, or anomalous activity that is aimed at disrupting the confidentiality, integrity, or availability of a protected network and its computer systems. Other tools can be used to monitor the activity of users within systems.

conduct manual or automated data review processes similar to those described by the exchanges. By reviewing and testing data prior to integrating patients' health information into electronic information exchange systems, the case study HIEs and providers are taking steps to ensure that the providers with which they exchange electronic personal heath information receive accurate and complete data about their patients.

HIEs and Providers Reported Similar Steps They Take to Establish Accountability for the Protection of Personal Health Information

The HIEs in our study described steps they take to hold individuals accountable for protecting patients' personal health information. All four exchanges stated that policies and procedures for the appropriate disclosure of health information and consequences for improper use of personal health information are included in agreements that HIEs establish with their participating providers prior to initiating health information sharing activities.[37] Specifically, exchanges described potential consequences for misuse of data by their participating providers and their employees, including suspending system access, terminating employment, and prosecuting criminal activities. All the case study exchanges stated that they maintain system access logs, which are reviewed periodically to identify inappropriate use or disclosure of data. Further, one exchange reported that its security officer performs reviews of providers' internal security and privacy policies and procedures to ensure that minimum protections are in place, such as mechanisms for obtaining patients' consent to share information, and that practices meet legal requirements.

Providers described similar practices for ensuring accountability. For example, all the providers with whom we spoke stated that they take steps such as training staff on privacy and security policies, requiring staff to document their understanding of the organization's privacy and security policies related to accessing and sharing personal health information, performing periodic audits of system access, and imposing penalties on users who violate policies. Seven providers require employees who access patients' information to sign agreements that state they will properly use

[37] HIEs and their participants typically establish agreements that govern how they will share and protect their patients' personal health information. The number and terms of data use agreements varied among our case studies. For example, one HIE stated that it required participants to sign agreements for each of the services it offered (e.g., one data use agreement for the delivery of laboratory results and another for patient information queries), while others established agreements that defined requirements for multiple services.

and disclose the information. One provider also reported additional practices, such as conducting physical inspections to ensure that workstations and records are properly secured and aligning staff bonuses with privacy and security compliance. Another provider reported that it improved its internal practices for ensuring accountability after it began participating in an HIE. In this case, the HIE had implemented audit functionalities in its system that were more robust than those in the provider's own system, which prompted the provider to modify its internal audit software.

The case study HIEs and providers reported that they implement practices they feel are necessary to ensure that the individuals to whom personal health information is disclosed are held accountable for safeguarding the information against improper use and disclosure. The steps that they described, such as training, automated and manual reviews of systems and data access, and penalties for improper use of information, are intended to prevent, identify, and correct situations in which personal health information are not being protected.

HIEs, Providers, and Other Entities Reported Examples of Ways the Electronic Sharing of Health Information Has a Positive Effect on the Quality of Care

Although the exchanges stated that they had not conducted formal studies of the effects of electronic sharing of personal health information on the quality of care their providers deliver, three of the HIEs reported examples of positive effects resulting from the services they provide.

- One of the exchanges reported that it provides alerts and reminders to participating providers regarding the health care of their patients, which can result in more timely interventions. An official from this exchange described one instance whereby a physician was reminded that seven of his patients needed colonoscopies based on exchange alerts he received for each patient. Because of these alerts, the physician notified the patients, and they received this procedure. Results of the tests identified important clinical information about three of the patients, and they were able to begin treatment.

- Two of these three exchanges provide a direct connection from participating hospitals to the state's Department of Public Health for real-time reporting of conditions and for supporting the early detection of disease outbreaks. According to an official with one of these exchanges, this service facilitated the state's ability to obtain information about cases of H1N1 more quickly than other states.

- Another exchange provides physicians with quality indicator reports based on clinical results from all participating institutions and physicians across the community. Specifically, physicians can create individualized reports based on patients for whom they are listed as the primary care physician for specific quality indicators, such as determining which patients have had a Pap smear in the last 3 years.

While none of the HIEs has conducted formal studies or otherwise evaluated the overall effect of the electronic sharing of health information on the quality of care, three of them discussed plans to study the effect of the electronic sharing of health information on specific aspects of health care quality.

- One exchange reported that it has started working with a local public health department to develop metrics based on prevalent health conditions in the community, such as the percentage of each provider's patients that have appropriate immunizations and the percentage of eligible patients that have had mammograms or other tests to screen for cancer. The exchange plans to aggregate some of its data to track these metrics and to study whether and how monitoring these metrics impacts the quality of care. An official at this HIE said that they intend to begin this initiative in 2010, but doing so is dependent on available funding.
- Another exchange reported that it initiated a quality improvement program in March 2009 that is intended to help physicians adhere to evidence-based medical practices to improve the health of their patients and to promote patient satisfaction. According to officials, this program merges claims data from health plans and clinical data from hospitals, laboratories, and physicians' offices. These data are used for metrics that target preventative care services and chronic disease management, including cancer screening, diabetic testing, and medications for those with asthma. Officials from this exchange stated that they have plans to study the effect of this program on the quality of care, but at the time of our review, they were not able to provide us with a time frame.
- A third HIE said that it has developed a plan to conduct an overall evaluation that will include analyzing how the electronic exchange of health information affects the quality of care, such as determining whether providers' use of the exchange has reduced the time it takes a provider to diagnose a patient because of easier access to information. Surveys and focus groups of providers who use data will be used to evaluate the effect of the exchange on the quality of care. Officials stated that they anticipate beginning this evaluation in 2010.

Additionally, the participating providers in our study—all of whom were identified as active users of an exchange—reported that, because they are part of an HIE, they have had more comprehensive and timely patient health information available at the point of care, which they believe has had a positive effect on the quality of care. Providers said that they can access information about their patients through their exchange that is not otherwise available in their own records, including information about medications and test results obtained from other providers, which gives them more comprehensive information about the status of their patients' health. Additionally, providers save time by obtaining patients' information from the exchange rather than by contacting other providers by fax or mail, or by repeating tests that other providers have already conducted, allowing for more timely information at the point of care. Some providers also told us that they use the HIE to obtain patient laboratory results more quickly than by the traditional methods of mail or fax, which has facilitated earlier intervention for patients. Participating providers gave us these additional examples of how they saw the information obtained through the exchange as having a positive effect on the quality of care for their patients:

- A large hospital reported that physicians in the emergency department have used the HIE to obtain medication information about patients, such as information about patients' medication allergies, to identify and avoid potential adverse drug interactions.

- A medium-sized hospital stated that information obtained through the HIE helped their emergency department physician ascertain that a patient who was requesting medication for pain had been in five area hospitals in seven nights seeking pain medication. The physician did not prescribe any pain medication for the patient.

- A small physician's practice and a large hospital reported that information available through the exchange facilitates the transfer of patients. Hospital officials said that by having immediate access to information on patients transferred to them, physicians can begin to develop treatment plans for the patient earlier, resulting in more timely care. Also, because they have access to the patients' test results, physicians at the receiving facility do not end up repeating tests that have already been performed.

- A participating physician from a family practice clinic reported that the HIE provided valuable information about a patient who had left the hospital before being treated. Information about this patient in the exchange revealed that emergency department physicians had been trying to reach the patient because he had been experiencing the initial signs of a heart attack. As a result of having this information, the physician sent this patient back to the hospital to be treated for cardiac arrest.

- Officials at a participating public health department stated that they use information obtained through the HIE to maintain their immunization and exam records for children, including exams that screen for vision, hearing, nutrition, or other issues. The officials reported that this information has helped to eliminate duplication of exams by the health department or private physicians, who may also conduct exams for these children.
- A large hospital from one of the exchanges reported that their cardiologist was able to obtain an abnormal laboratory result electronically from their exchange one day before they would have without using it, allowing earlier intervention for a potentially life-threatening condition.

Two of the other entities we interviewed—integrated health care delivery systems that share information within their own systems—reported that they have joined or have considered joining an HIE to obtain more comprehensive information about their patients, who may obtain health care services from providers outside of their systems. Officials with one of the integrated health care systems said that they joined an exchange recently because they felt it would provide physicians and other health care providers with a more complete picture of a patient's health information regardless of where the patient obtains care, which could help to eliminate unnecessary or duplicative care, including tests that may have already been performed by other providers. Officials from the second integrated health care delivery system told us that they were considering joining an exchange because it could provide them with information about care—such as medications prescribed—obtained from providers outside of their system. In addition, these officials noted that joining the exchange could benefit emergency department physicians by helping them obtain immediate, more comprehensive information about patients.

If you have any questions on matters discussed in this report, please contact me at (202) 512-6304, Gregory C. Wilshusen at (202) 512-6244, or Linda T. Kohn at (202) 512-7114, or by e-mail at melvinv@gao.gov, wilshuseng@gao.gov, or kohnl@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.

Valerie C. Melvin

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

Linda T. Kohn

Linda T. Kohn
Director, Health Care

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

List of Committees

The Honorable Tom Harkin
Chairman
The Honorable Michael B. Enzi
Ranking Member
Committee on Health, Education, Labor,
and Pensions
United States Senate

The Honorable Henry A. Waxman
Chairman
The Honorable Joe Barton
Ranking Member
Committee on Energy and Commerce
House of Representatives

The Honorable Pete Stark
Chairman
The Honorable Wally Herger
Ranking Member
Subcommittee on Health
Committee on Ways and Means
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to describe (1) the practices implemented for disclosing personal health information for purposes of treatment, including the use of electronic means for obtaining consent, as reported by selected health information exchanges, their participating providers, and other entities; and (2) the effects of the electronic sharing of health information on the quality of care for patients as reported by these organizations.

To address both objectives, we conducted case studies of selected health information exchanges and their participating providers. We selected four operational health information exchanges and a sample of participating providers for each of the four exchanges. To select the case study health information exchanges, we compiled a list of 68 health information exchanges that were reported to be operational and actively sharing data among providers.[1] From this list, we selected a judgmental, non-generalizable sample of four exchanges. Each exchange we selected met two of the following three characteristics:

- had an interstate data exchange and the need to address different state laws and regulations applicable to the disclosure of protected health information;
- included varying numbers, sizes, and types of provider organizations that disclose health information through the exchange; and
- operated with some degree of state involvement such as a state-led or state-level health information exchange.

To identify exchanges with the selected characteristics, we reviewed our prior reports, and reports on outcomes of relevant Department of Health and Human Services projects such as the Nationwide Health Information Network, the State-level Health Information Exchange Consensus Project,

[1] We compiled this list based on data obtained from published research, the Department of Health and Human Services' Office of the National Coordinator for Health Information Technology, and our prior work on electronic health information exchange (see GAO-07-238). We did not validate the information derived from our analysis of these data.

and the Health Information Security and Privacy Collaboration.[2] We also reviewed published research identifying active health information exchanges and relevant policy issues, and research published by health information technology professional associations and other health information privacy experts having data and knowledge about active health information exchange organizations. Finally, we considered the geographic location of the exchanges when making our final selection.

We worked with each health information exchange to select a judgmental sample of participating providers. The categories of providers we used to ensure that we would have a variety in our sample included:

- small and medium hospitals with 199 beds or fewer;
- large hospitals with 200 beds or more;
- small physician practices with fewer than 10 full-time equivalent employees;
- large physician practices that have 10 or more full-time equivalent employees; and
- other types of organizations, including long-term care facilities, public health facilities, pharmacies, laboratories, and insurance plans.

We were unable to include all categories of participating providers for each exchange in our sample because some exchanges did not include providers from each category. We studied various types of providers that were active users of health information exchanges and that shared information directly with other providers (that are not members of the exchange). Because each health information exchange defined parameters for and tracked usage of the exchanges differently, we relied on officials

[2] Since 2005, the Office of the National Coordinator for Health Information Technology has established a number of initiatives to address privacy and security in planning to promote nationwide health information exchange. The Nationwide Health Information Network project is intended to define standards, protocols, legal agreements, specifications, and services needed to develop a common platform for secure health information exchange across the country. The State-level Health Information Exchange Consensus Project was created to provide a forum for the Office of the National Coordinator to work with state partners to align state-based health information exchange activities with a national health information technology agenda. The Health Information Security and Privacy Collaboration brought together 42 states and territories to address the privacy and security challenges presented by electronic health information exchange.

from each exchange to identify providers from each category that were active users of the HIE's services.

For each of the four case studies, we

- gathered documentation and conducted interviews with the exchanges to determine the practices they implemented for disclosing personal health information, including electronic means of obtaining consent, practices they required for participating providers, and reported effects of sharing health information electronically on the quality of care; and
- gathered documentation and conducted interviews with officials from selected participating providers to determine the practices they implemented as part of the health information exchange and the practices they had implemented in their own organization for disclosing personal health information. In addition, we interviewed officials from these participating providers to determine how and to what extent the electronic sharing of health information affected the quality of care.

At the conclusion of our study, we validated the information that we included in this report with the exchanges and providers to confirm that their disclosure practices and examples of the effects of electronic sharing of personal health information were accurately portrayed. While we did not independently test the reported practices and examples of effects on quality of care, we corroborated the testimonial evidence obtained during our case studies with supporting documentation.

For additional information about the health information exchanges and participating providers we studied, see appendix II.

To supplement the information we obtained from our case studies, we gathered information from and conducted interviews with other entities, including two integrated health care delivery systems. We also held discussions with two professional associations (eHealth Initiative and Healthcare Information Management and Systems Society) and 11 of their affiliated health information exchanges, and the New York eHealth Collaborative, an organization focused on developing and enforcing New York State's health information exchange policy. We interviewed and obtained additional information from other health care organizations, including the American Hospital Association, the Agency for Healthcare Research and Quality, the American Medical Association, and the Center for Studying Health System Change. Additionally, we reviewed federal requirements for protecting electronic personal health information, accepted privacy guidelines produced by the Organization for Economic Cooperation and Development and the Markle Foundation's Connecting for Health Collaborative, and reports and guidance on implementing privacy practices produced by the Department of Health and Human Services' Office for Civil Rights and Office of the National Coordinator for Health Information Technology. We also interviewed privacy experts from the Health Policy Institute at Georgetown University and the World Privacy Forum.

We conducted our work from May 2009 to February 2010 in accordance with all sections of GAO's Quality Assurance Framework that are relevant to our objectives. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations in our work. We believe that the information and data obtained, and the analysis conducted, provide a reasonable basis for any findings and conclusions.

Appendix II: Case Studies

Case Study 1

Unlike other case studies, this exchange stores all information it shares in a central repository. However, the exchange stores each provider's data separately and only allows providers to obtain information from the HIE about patients from the point in time when that provider began treating the patient.

Case Study 1 was of a health information exchange (HIE) serving a metropolitan area and a neighboring state. The HIE was organized in 1995 by a private company and has supported the exchange of health information among providers in its metropolitan area and neighboring state since 2006. For this case study, we identified disclosure practices reported by the HIE, two of its participating hospitals, and three provider practices.

Providers participating in the exchange	Number of providers
Small hospitals	3
Large hospitals	3
Small provider practices	
General practitioner	42
Specialist	52
Large provider practices	
General practitioner	5
Specialist	11
Other (e.g., clinical laboratories, long-term care facilities, hospices, etc.)	11

Source: GAO analysis of case study data.

The tools and services offered by this HIE include:

- Delivery of results to providers via an online inbox (e.g., laboratory test results)
- Communications (e.g., messaging for sending, receiving and managing information about patients among providers)
- Access by emergency department physicians to clinical history from all participating providers for patients being treated in emergency departments
- Electronic health record system for providers opting to store their patient records with the HIE instead of in internal systems
- Assistance to providers with technology implementation and training as well as provider-specific analysis of patient data for quality review purposes

Table 1 describes the methods of implementing disclosure practices reported by the HIE and the five participating providers that we studied.

Table 2: Case Study 1 Reported Practices for Disclosing Personal Health Information

HIE 1	Provider 1 Large hospital	Provider 2 Large hospital	Provider 3 Large general physician practice	Provider 4 Large specialty physician practice	Provider 5 Small physician office
Informing individuals about the uses of their information and how it will be protected					
N/A[a]	• Provides paper notices • Posts notice on Web site • Does not notify of HIE	• Provides paper notices • Posts notice on Web site • Does not notify of HIE	• Provides paper notices • Posts notice on Web site • Does not notify of HIE	• Provides paper notices • Posts notice on Web site • Does not notify of HIE	• Provides paper notices • Does not notify of HIE
Obtaining individual consent					
N/A	• Obtains written consent • Does not include consent for sharing patients' information through the HIE	• Obtains written consent • Does not include consent for sharing patients' information through the HIE	• Obtains written consent • Does not include consent for sharing patients' information through the HIE	• Obtains written consent • Does not include consent for sharing patients' information through the HIE	• Obtains written consent • Does not include consent for sharing patients' information through the HIE
Facilitating individual access to and correction of electronic medical records					
N/A	• Includes additions to record if patient request is approved	• Allows patients to view records via Web portal • Includes additions to record if patient request is approved	• Allows patients to view records in office • Includes additions to record if patient request is approved	• Includes additions to record if patient request is approved	• Includes additions to record if patient request is approved

HIE 1	Provider 1 Large hospital	Provider 2 Large hospital	Provider 3 Large general physician practice	Provider 4 Large specialty physician practice	Provider 5 Small physician office
Limiting the use and disclosure of personal medical information to a specific purpose					
• Implements role-based access controls • Limits disclosure to patients' summary data • Limits secondary use limited to public health reporting • Retains electronic health records indefinitely	• Implements role-based access controls • Requires application and data owners to approve staff access to certain data • Reviews requests and limits data shared • Limits data provided to last 10 years • Limits secondary use to public health reporting and emergency room research	• Implements role-based access controls • Limits secondary use to public health reporting and emergency room research	• Implements role-based access controls • Reviews requests and verifies identity of requester before sharing data • Limits secondary use to public health reporting, internal quality analysis, and to train staff	• Implements role-based access controls • Specifies data to disclose for different uses and purposes • Retains electronic health records indefinitely • Purges large image files after 7 years	• Implements role-based access controls • Allows patient to specify full or partial release of records • Limits information sent to specialists • Retains electronic health records indefinitely

HIE 1	Provider 1 Large hospital	Provider 2 Large hospital	Provider 3 Large general physician practice	Provider 4 Large specialty physician practice	Provider 5 Small physician office
Providing security safeguards					
Access controls: • Limits provider access to patients' data back to first patient visit • Registers and approves users • Requires username and password for system access • Requires additional authentication for system access • Technical safeguards: • Encryption • Secure point-to-point connections • Firewalls • Alternate network in case of system failure • Offsite backup of system data	Access controls: • Registers and approves users • Requires username and password for system access • Ends link to patient record with system logoff Technical safeguards: • Encryption • Firewalls • Intrusion detection • System time outs	Access controls: • Registers and approves users • Requires username and password for system access Technical safeguards: • Secure connection through virtual private network • Encryption • Firewalls • Intrusion detection	Access controls: • Registers and approves users • Requires username and password for system access Technical safeguards: • System time outs	Access controls: • Registers and approves users • Requires username and password for system access • Requires additional authentication for system access by remote users Technical safeguards: • Encryption	Access controls: • Registers and approves users • Requires username and password for system access • Requires additional authentication for system access by remote users Technical safeguards: • Direct connection to HIE system • Encryption • Firewalls • System time outs
Ensuring that data are accurate, timely, and complete					
• Verifies data quality during system interface tests • Conducts manual data reviews	• Verifies identity of patients through automated tools	• Verifies data quality during system interface tests • Conducts automated and manual data reviews	• None reported	• Conducts manual data reviews	• Verifies data quality during system interface tests • Conducts manual data reviews

HIE 1	Provider 1 Large hospital	Provider 2 Large hospital	Provider 3 Large general physician practice	Provider 4 Large specialty physician practice	Provider 5 Small physician office
Establishing accountability for how personal information is protected					
• Reviews providers' privacy policies • Audits system access	• Requires employees to sign agreements for proper use and disclosure • Audits system access	• Requires employees to sign agreements for proper use and disclosure • Implements policy for sanctioning employees for improper use • Audits system access	• Implements policy for sanctioning employees for improper use • Audits system access	• Audits system access	• Requires employees to sign agreements for proper use and disclosure • Implements policy for sanctioning employees for improper use • Audits system access

Source: GAO analysis of case study data.

[a] HIEs are not in contact with patients and do not address the first three practices.

Case Study 2

This HIE has developed an electronic tool that providers use to record patient consent. Its system requires participating providers to indicate patient consent before patient information is accepted for sharing among its participants. Providers are required to select options at each patient visit, and the system manages sharing of patients' records automatically based on the options selected. For example, if the provider's entry indicates that a patient did not consent to sharing information about a visit, the system would not accept or provide other providers access to that information. However, if the entry indicated that the patient consented to sharing information, the health information recorded from that visit would be made available through the HIE to all participating providers.

Case Study 2 was of an HIE that serves multiple states. The HIE is led by a nonprofit organization and supports regional level information exchange. Organized in 2005, this HIE began actively exchanging data among its participating providers in 2008. For this case study, we identified disclosure practices reported by the HIE, a hospital, two provider practices, and a public health department.

Providers participating in the exchange	Number of providers
Small hospitals	0
Large hospitals	1
Small provider practices	
General practitioner	1
Specialist	0
Large provider practices	
General practitioner	1
Specialist	1
Other (e.g., health plan, public health department)	2

Source: GAO analysis of case study data.

Note: The HIE has eight additional providers currently building interfaces to actively exchange data, including a small hospital, small provider practice, large provider practices, and others (e.g., clinical laboratory).

The tools and services offered by the HIE include:

- Communications (e.g., receiving and managing information about patients among providers)
- Interface to support searching for patient data by providers and presenting data in a standard summary medical record format
- Assistance to providers with technology implementation and training as well as provider-specific analysis of patient data for quality review purposes

Table 2 describes the methods of implementing disclosure practices reported by the HIE and the four participating providers that we studied.

Table 3: Case Study 2 Reported Practices for Disclosing Personal Health Information

HIE 2	Provider 1 Large hospital	Provider 2 Large provider practice	Provider 3 Small provider practice	Provider 4 Public health department
Informing individuals about the uses of their information and how it will be protected				
• N/A[a]	• Provides paper notices • Notifies patients of HIE • Posts notice on Web site	• Provides paper notices • Does not notify of HIE • Posts notice on Web site	• Provides paper notices • Notice of privacy practices includes HIE	• Provides paper notices • Notice of privacy practices includes HIE
Obtaining individual consent				
• N/A	• Obtains written consent • Consent recorded electronically • Patients opt in for sharing their information through the HIE	• Obtains written consent • Consent recorded electronically • Patients can opt out of sharing their information through the HIE	• Obtains written consent • Consent recorded electronically • Patients can opt out of sharing their information through the HIE	• Obtains written consent • Consent recorded electronically • Patients can opt out of sharing their information through the HIE
Facilitating individual access to and correction of electronic medical records				
• N/A	• Includes addition to record if patient request to amend is approved	• Allows patients to view records via Web portal • Includes addition to record if patient request to amend is approved	• Allows patients to view records in office • Includes addition to record if patient request to amend is approved	• Includes addition to record if patient request to amend is approved
Limiting the use and disclosure of personal medical information to a specific purpose				
• Implements role-based access controls • Limits disclosure to patients' summary data • Retains electronic health records while business relationship exists and 3 years following that relationship	• Implements role-based access controls • Reviews requests and limits data shared • Retains electronic health records based on the type of data contained; potentially retained indefinitely	• Implements role-based access controls • Reviews requests and limits data shared • Limits secondary use to internal quality analysis • Retains electronic health records indefinitely	• Implements role-based access controls • Limits the sharing of sensitive information • Does not allow secondary use of data • Retains electronic health records indefinitely	• Limits secondary use to population health research • Retains electronic health records indefinitely

HIE 2	Provider 1 Large hospital	Provider 2 Large provider practice	Provider 3 Small provider practice	Provider 4 Public health department
Providing security safeguards				
Access controls: • Limits provider access to patients' data to the original provider • Registers and approves users • Requires username and password for system access • Requires additional authentication for system access • Technical safeguards: • Encryption • Secure connections through virtual private network • Offsite backup of system data	Access controls: • Registers and approves users • Requires username and password for system access • Requires additional authentication for system access • Technical safeguards: • Encryption • Firewalls • Intrusion detection	Access controls: • Registers and approves users • Requires username and password for system access • Technical safeguards: • Secure connections through virtual private network • Encryption	Access controls: • Registers and approves users • Requires username and password for system access • Technical safeguards: • System timeouts • Secure connections through virtual private network, • Secure connections for remote access • Encryption • Firewalls	Access controls: • Registers and approves users • Requires username and password for system access • Technical safeguards: • Secure connections through virtual private network • Encryption • Firewalls
Ensuring that data are accurate, timely, and complete				
• Verifies data quality during system interface tests • Conducts manual data reviews • Verifies identity of patient through automated tools	• Verifies data quality during system interface tests • Conducts manual data reviews	• Conducts automated data reviews	• Verifies data quality during system interface tests	• Conducts manual data reviews
Establishing accountability for how personal information is protected				
• Reviews providers' privacy policies • Audits system access	• Implements policy for sanctioning employees for improper use • Audits system access	• Requires employees to sign agreements for proper use and disclosure • Implements policy for sanctioning employees for improper use • Audits system access	• Audits system access	• Audits system access

Source: GAO analysis of case study data.

[a]HIEs are not in contact with patients and do not address the first three practices.

Case Study 3

This HIE works with providers and vendors to establish and certify interfaces for electronic health record systems. All providers using a vendor's electronic health record software must use the certified interface to connect to the HIE.

Case Study 3 was of an HIE serving one state. Operated by a public-private partnership, the exchange was created by state statute in 1997 and began supporting the exchange of health information among providers in May 2007. The participating providers selected for review as part of this case study included two hospitals and two provider practices.

Providers participating in the exchange	Number of providers
Hospitals	6
Provider practices (e.g., private physician practices, health centers, hospital emergency departments, clinics)	144
Other (e.g., two national clinical laboratories, pathology provider)	5

Source: GAO analysis of case study data.

The tools and services offered by this HIE include:

- Secure delivery of clinical results in a standardized format (e.g., laboratory test results), reports (e.g., radiology), and face sheets (demographic and billing information)
- Searchable clinical history
- Enhanced provider-to-provider communication (e.g., forwarding clinical results to HIE users' inbox)
- Interface to support searching for patient data in electronic health record for those providers with them
- Interface for public health reporting and biosurveillance activities

Table 3 describes the methods of implementing disclosure practices reported by the HIE and the four participating providers that we studied.

Table 4: Case Study 3 Reported Practices for Disclosing Personal Health Information

HIE 3	Provider 1 Large hospital	Provider 2 Small hospital	Provider 3 Large specialty physician practice	Provider 4 Small physician practice
Informing individuals about the uses of their information and how it will be protected				
• N/A[a]	• Provides paper notices • Posts notice on Web site • Does not notify of HIE	• Provides paper notices • Posts notice on Web site • Does not notify of HIE	• Provides paper notices • Posts notice on Web site • Notifies of participation in HIE	• Does not notify of HIE
Obtaining individual consent				
• N/A[b]	• Obtains written consent • Does not include consent for sharing information through the HIE	• Obtains written consent • Allows patients to opt out of sharing information through the HIE	• Obtains written consent	• Obtains written consent • Allows patients to opt out of sharing patients' information through the HIE
Facilitating individual access to and correction of electronic medical records				
• N/A	• Includes addition to record if patient request to amend is approved	• Allows patients to view records via Web portal • Includes addition to record if patient request to amend is approved	• Includes addition to record if patient request to amend is approved	• Includes addition to record if patient request to amend is approved
Limiting the use and disclosure of personal medical information to a specific purpose				
• Implements role-based access controls • Limits secondary use limited to public health reporting • Does not retain patient clinical data	• Implements role-based access controls • Reviews requests and limits data shared on a case-by-case basis • Limits data provided to last 10 years • Limits secondary use to public health reporting and emergency room research	• Implements role-based access controls • Limits secondary use to public health reporting, internal quality analysis, and emergency room research	• Implements role-based access controls • Limits secondary use to internal quality analysis • Retains electronic health records indefinitely	• Implements role-based access controls • Limits secondary use to internal quality analysis • Retains electronic health records indefinitely

HIE 3	Provider 1 Large hospital	Provider 2 Small hospital	Provider 3 Large specialty physician practice	Provider 4 Small physician practice
Providing security safeguards				
Access controls: • Requires username and password for system access • Requires providers to request and justify access to information to HIE patient data from other providers Technical safeguards: • Secure connections through virtual private network • Firewalls • Red flags for repeat requests for access to HIE patient data from other providers	Access controls: • Registers and approves users • Requires username and password for system access • Ends link to patient record with system logoff Technical safeguards: • System time outs • Secure connection through virtual private network for remote access • Firewalls	• Access controls: • Registers and approves users • Requires username and password for system access Technical safeguards: • Secure connection through virtual private network • Encryption • Firewalls • System time outs • Physical security controls, such as walk-arounds to identify improperly secured workstations	Access controls: • Requires username and password for system access • Ability to lock selected records Technical safeguards: • Firewalls • Secure connection through virtual private network	Access controls: • Registers and approves users • Requires two sets of username and password for system access Technical safeguards: • Secure connection through virtual private network • Encryption • Firewalls • System timeouts
Ensuring that data are accurate, timely, and complete				
• Verifies data quality during system interface tests • Conducts manual data reviews • Verifies identity of patient through automated tools	• Requires staff to sign off for quality of data entered into system • Uses automated tool to identify duplicate records	• Verifies data quality during system interface tests	• None reported (does not yet actively share data)	• Conducts manual data reviews

HIE 3	Provider 1 Large hospital	Provider 2 Small hospital	Provider 3 Large specialty physician practice	Provider 4 Small physician practice
Establishing accountability for how personal information is protected				
• Audits system access • Requests providers to notify of violations	• Conducts internal security audits	• Requires employees to sign agreements for proper use and disclosure • Implements policy for sanctioning employees for improper use • Audits system access	• Segregates duties • Audits system access	• Implements policy for sanctioning employees for improper use • Audits system access

Source: GAO analysis of case study data.

[a] HIEs are not in contact with patients and do not address the first three practices.

[b] If patients choose to not have information shared through the exchange, providers direct them to the HIE's Web site for forms which, when signed and notarized, authorize the HIE to restrict providers' ability to search for the patients' information.

Case Study 4

This exchange normalizes or converts the data providers submit to the exchange into a common format by applying nationally recognized health information technology standards. For example, the exchange provides laboratory test result data using logical observation identifiers names and codes (LOINC®) standards approved by the Department of Health and Human Services for use in sharing health information. This exchange also provides a quality reporting program to providers who enroll, gathering data collected from various HIE services to develop quality metrics to aid those providers in assessing their practices.

Case Study 4 was of an HIE serving one state. The HIE was established as a public-private partnership led by a nonprofit organization in 2004. It supports state-level information exchange and began actively exchanging data amongst its participating providers in 2007. For this case study, we identified disclosure practices reported by the HIE, two hospitals, a physician practice, and two clinics.

Providers participating in the exchange[a]	Number of providers
Hospitals	39
Provider practices	4,240
Other (e.g., clinics and state and local health departments)	4

Source: GAO analysis of case study data.

[a] We did not report detailed information about the size and type of provider practices because this HIE does not maintain that information.

The tools and services offered by this exchange include:

- Delivery of results to providers (e.g., laboratory test results)
- Communications (e.g., messaging for sending, receiving and managing information about patients among providers)
- Automatic delivery of patients' clinical history from all participating providers to emergency departments when patients are registered
- Quality metrics based upon analysis of provider data for key indicators (e.g., mammograms provided to patients for whom they are indicated)
- Interface to support reporting by hospitals of reportable conditions and emergency department chief complaint data to state health department

Table 4 describes the methods of implementing disclosure practices reported by the HIE and five of its participating providers that we studied.

Table 5: Case Study 4 Reported Practices for Disclosing Personal Health Information

HIE 4	Provider 1 Large hospital	Provider 2 Medium hospital	Provider 3 Large specialty physician practice	Provider 4 Other (university affiliated clinic)	Provider 5 Other (federal qualified clinic)
Informing individuals about the uses of their information and how it will be protected					
N/A[a]	• Provides paper notices • Posts notice on Web site • Notifies patients of HIE	• Provides paper notices • Posts notice on Web site • Does not notify of HIE	• Provides paper notices • Posts notice on Web site • Does not notify of HIE	• Provides paper notices • Posts notice on Web site • Does not notify of HIE	• Provides paper notices • Does not notify of HIE
Obtaining individual consent					
N/A	• Obtains written consent • Does not include consent for sharing patients' information through the HIE	• Obtains written consent • Does not include consent for sharing patients' information through the HIE	• Obtains written consent • Does not include consent for sharing patients' information through the HIE	• Obtains written consent • Does not include consent for sharing patients' information through the HIE	• Obtains written consent on paper • Does not include consent for sharing patients' information through the HIE
Facilitating individual access to and correction of electronic medical records					
N/A	• Includes addition to record if patient request to amend is approved	• Includes addition to record if patient request to amend is approved	• Includes addition to record if patient request to amend is approved	• Includes additions to record if patient request to amend is approved	• Includes additions to record if patient request to amend is approved

HIE 4	Provider 1 Large hospital	Provider 2 Medium hospital	Provider 3 Large specialty physician practice	Provider 4 Other (university affiliated clinic)	Provider 5 Other (federal qualified clinic)
Limiting the use and disclosure of personal medical information to a specific purpose					
• Implements role-based access controls • Can limit disclosure to patients' summary data upon provider request • Limits secondary use to internal quality analysis, public health reporting and approved clinical research • Retains electronic health records indefinitely	• Implements role-based access controls • Limits secondary use to internal quality analysis, public health reporting, and approved clinical research • Retains electronic health records indefinitely	• Implements role-based access controls • Limits secondary use to public health reporting and approved research • Retains electronic health records indefinitely	• Implements role-based access controls • Limits secondary use to approved research • Retains electronic health records indefinitely	• Implements role-based access controls • Limits secondary use to internal quality analysis • Retains electronic health records indefinitely	• Implements role-based access controls • Limits secondary use to internal quality analysis, public health reporting, and approved research • Retains electronic health records indefinitely

HIE 4	Provider 1 Large hospital	Provider 2 Medium hospital	Provider 3 Large specialty physician practice	Provider 4 Other (university affiliated clinic)	Provider 5 Other (federal qualified clinic)
Providing security safeguards					
Access controls: • Returns data after five unsuccessful attempts to deliver patient results • Registers and approves users • Requires username and password for system access • Requires additional authentication for system remote access Technical safeguards: • Secure connection through virtual private network • Firewalls • Passwords expire after certain time • Remote access not permitted for certain applications	Access controls: • Registers and approves users • Requires username and password for system access Technical safeguards: • Secure connection through virtual private network • Firewalls	Access controls: • Registers and approves users • Requires username and password for system access • Requires additional authentication for system remote access Technical safeguards: • Secure connection through virtual private network • Encryption • Firewalls • Separate wireless connections for Internet and intranet access	Access controls: • Registers and approves users • Requires username and password for system access Technical safeguards: • Secure connection through virtual private network • System timeouts • Passwords expire after certain time	Access controls: • Registers and approves users • Requires username and password for system access • Required additional authentication for remote system access Technical safeguards: • Secure connection through virtual private networks • Encryption • Firewalls • System timeouts	Access controls: • Registers and approves users • Requires username and password for system access • Requires additional authentication for system remote access Technical safeguards: • Secure connection through virtual private network for remote system access • System timeouts • Firewalls • Encryption • Physical security controls, such as shutting down workstations in exam rooms after use

HIE 4	Provider 1 Large hospital	Provider 2 Medium hospital	Provider 3 Large specialty physician practice	Provider 4 Other (university affiliated clinic)	Provider 5 Other (federal qualified clinic)
Ensuring that data are accurate, timely, and complete					
• Verifies data quality during system interface tests • Maps data from providers' systems to national standards for storage and use in HIE • Verifies identity of patient through automated tools • Conducts manual data reviews	• Conducts manual data reviews	• Conducts manual data reviews	• Conducts manual data reviews	• Conducts manual data reviews	• Conducts manual data reviews
Establishing accountability for how personal information is protected					
• Requires providers and employees to sign agreements for use and disclosure • Requests that providers notify of violations • Audits system access	• Requires employees to sign agreements for use and disclosure • Implements policies for sanctioning employees for improper use • Audits system access	• Implements policies for sanctioning employees for improper use • Audits system access	• Implements policies for sanctioning employees for improper use • Audits system access	• Parent health organization privacy officer conducts compliance reviews • Audits system access	• Requires employees to sign agreements for use and disclosure • Implements policies for sanctioning employees for improper use

Source: GAO analysis of case study data.

[a] HIEs are not in contact with patients and do not address the first three practices.

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Valerie C. Melvin (202) 512-6304 or melvinv@gao.gov
Linda T. Kohn (202) 512-7114 or kohnl@gao.gov
Gregory C. Wilshusen (202) 512-6244 or wilshuseng@gao.gov

Acknowledgments

In addition to the contacts named above, key contributors to this report were Bonnie W. Anderson (Assistant Director), John A. de Ferrari (Assistant Director), Teresa F. Tucker (Assistant Director), Monica Perez Anatalio, Danielle A. Bernstein, April W. Brantley, Susan S. Czachor, Neil J. Doherty, Rebecca E. Eyler, Amanda C. Gill, Nancy E. Glover, Ashley D. Houston, Fatima A. Jahan, Thomas E. Murphy, and Terry L. Richardson.

(310939)

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 afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

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