United States Government Accountability Office

GAO

Report to the Chairman, Committee on Health, Education, Labor, and Pensions, U.S. Senate

September 2004

HEALTH INFORMATION

First-Year Experiences under the Federal Privacy Rule

GAO-04-965

September 2004

HEALTH INFORMATION

First-Year Experiences under the Federal Privacy Rule

GAO Highlights

Highlights of GAO-04-965, a report to the Chairman, Committee on Health, Education, Labor, and Pensions, U.S. Senate.

Why GAO Did This Study

Issued under the Health Insurance Portability and Accountability Act of 1996, the Privacy Rule provided new protections regarding the confidentiality of health information and established new responsibilities for providers, health plans, and other entities to protect such information. GAO reviewed (1) the experience of providers and health plans in implementation; (2) the experience of public health entities, researchers, and representatives of patients in obtaining access to health information; and (3) the extent to which patients appear to be aware of their rights.

What GAO Recommends

GAO recommends that HHS (1) require that patients be informed of mandatory disclosures to public health authorities in privacy notices and exempt such disclosures from the accounting requirement, and (2) conduct a public information campaign to improve patients' awareness of their rights. HHS noted that it continues to monitor the public's experience with the accounting provision to assess the need to modify the rule and described ongoing efforts to educate consumers. GAO remains concerned about the burden of accounting for disclosures to public health authorities and believes it is important that HHS more effectively disseminate information about the Privacy Rule.

www.gao.gov/cgi-bin/getrpt?GAO-04-965.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Leslie G. Aronovitz at (312) 220-7600.

What GAO Found

Organizations representing providers and health plans told us that implementation of the Privacy Rule went more smoothly than expected during the first year after most entities were required to be compliant. In addition, they reported that new privacy procedures have become routine practice for their members' staff. However, provider and health plan representatives also raised a variety of issues about provisions that continue to be problematic. In particular, many organizations emphasized that two provisions—the requirement to account for certain information disclosures and the requirement to develop agreements with business associates that extend privacy protections "downstream"—are unnecessarily burdensome. Some organizations suggested that difficulties with these provisions could be ameliorated with modification of certain provisions and further guidance from the Department of Health and Human Services' Office for Civil Rights (OCR).

Organizations reported a number of challenges faced by entities that rely on access to health information for public health monitoring, research, and patient advocacy. Public health entities noted that some states have had to take concerted action to ensure that providers' concerns about complying with the Privacy Rule do not impede the flow of important information to state health departments and disease registries. Some research groups asserted that the rule has delayed clinical and health services research by reducing access to data. Some consumer advocacy groups told us that patients' families, friends, and other representatives have experienced unnecessary difficulty in assisting patients. These groups perceived that while providers and plans are allowed, in certain cases, to disclose health information without written patient authorization, they are reluctant to do so.

Consumer and provider representatives contend that the general public is not well informed about their rights under the Privacy Rule. According to these organizations, patients may not understand the privacy notices they receive, or do not focus their attention on privacy issues when the notices are presented to them. Some evidence of patients' lack of understanding is reflected in the 5,648 complaints filed with OCR in the first year after the Privacy Rule took effect. Of the roughly 2,700 complaint cases OCR closed as of April 13, 2004, nearly two-thirds were found to fall outside the scope of the Privacy Rule because they either involved accusations of actions that were not prohibited by the regulation, involved entities that were not "covered entities" as defined by the Privacy Rule, or involved actions that occurred before covered entities were required to be compliant. Of those cases that were germane to the rule, OCR determined that about half represented cases in which no violation had occurred.

Contents

Abbreviations

AHCA	American Health Care Association
AHIMA	American Health Information Management Association
AHIP	America's Health Insurance Plans
APhA	American Pharmacists' Association
BCBSA	Blue Cross Blue Shield Association
CDC	Centers for Disease Control and Prevention
CMS	Centers for Medicare & Medicaid Services
CSTE	Council of State and Territorial Epidemiologists
FAQ	frequently asked question
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
IRB	institutional review board
JCAHO	Joint Commission on the Accreditation of Healthcare Organizations
MGMA	Medical Group Management Association
NCVHS	National Committee on Vital and Health Statistics
OCR	Office for Civil Rights

GAO
Accountability * Integrity * Reliability

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

September 3, 2004

The Honorable Judd Gregg
Chairman
Committee on Health, Education, Labor, and Pensions
United States Senate

Dear Mr. Chairman:

Issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the federal Privacy Rule provided individuals with new protections regarding the confidentiality of their health information and established new responsibilities for health care providers, health plans, and other entities to protect such information.[1] The rule was implemented as a result of advances in information technology and an increased number of parties with access to identifiable health information. Together, these trends have created new challenges to maintaining the privacy of an individual's medical records.

April 14, 2004, marked the first anniversary of the date that most entities were required to be compliant with the Privacy Rule. More than a full year of experience with the rule offers an important and timely opportunity to determine how different groups have fared under the new regulation. This report focuses on (1) the experience of providers and health plans in implementing the Privacy Rule; (2) the experience of public health entities, researchers, and representatives of patients in obtaining access to health information under the rule; and (3) the extent to which patients appear to be aware of their rights.

In gathering this information, we interviewed representatives of 23 national organizations representing health care consumers, health care providers, health plans, state officials, public health agencies, researchers, privacy professionals, and a health care accrediting body. (These organizations are listed in app. I.) We supplemented our discussions with these organizations with a review of information from their Web sites and surveys and reports issued by them. We also contacted the Centers for Disease Control and

[1] Pub. L. No. 104-191, § 264, 110 Stat. 1936, 2033. Additionally, HIPAA's administrative simplification provisions are aimed at encouraging the electronic transfer of health information and require the development of standards for electronic transactions, including standards for unique identifiers, code sets, and security. See §§ 261 and 262, 110 Stat. at 2021-2031.

Prevention (CDC)—a federal public health agency—and the Centers for Medicare & Medicaid Services (CMS)—the agency that administers the Medicare program—both in the Department of Health and Human Services (HHS). In addition, we spoke with officials at the Office for Civil Rights (OCR) within HHS—the agency responsible for enforcing the Privacy Rule—about their procedures for logging in privacy complaints and analyzed data extracted for us by OCR from the database that it maintains on these complaints. We did not independently verify the reliability of the data compiled by OCR. However, we determined that these data were sufficiently reliable for the purposes of our engagement. In addition, we reviewed testimony by public health and research organizations delivered at 2003 and 2004 hearings on the Privacy Rule held by the National Committee on Vital and Health Statistics (NCVHS) and followed up with several state officials.[2] We performed our work from March 2004 through August 2004 in accordance with generally accepted government auditing standards.

Results in Brief

Organizations representing providers and health plans told us that implementation of the Privacy Rule went more smoothly than expected during the first year. In addition, they reported that initial confusion has diminished and new privacy procedures have become routine practice for their members' staff. However, they noted ongoing difficulties with certain provisions and some remaining misunderstandings. In particular, many organizations emphasized that two provisions—the requirement to account for certain information disclosures and the requirement to develop agreements with business associates that extend privacy protections "downstream"—are unnecessarily burdensome. Some organizations suggested that difficulties with these provisions could be ameliorated with modification of certain provisions and further guidance from OCR.

Organizations reported a number of challenges faced by entities that rely on access to health information for public health monitoring, research, and patient advocacy. Public health entities noted that some states have had to take action to ensure that providers' concerns about complying with the Privacy Rule do not impede the flow of important information to state health departments and disease registries. Some research groups asserted

[2] NCVHS is an 18-member committee of individuals in the private sector that serves as the statutory public advisory body to the Secretary of HHS in the area of health data and statistics.

that the rule has delayed clinical and health services research by reducing access to data. Some consumer advocacy groups told us that patients' families, friends, and other representatives have experienced unnecessary constraints in assisting patients. They perceived that while providers and plans are allowed, in certain cases, to disclose health information without written authorization, they are reluctant to do so.

Representatives of provider and consumer groups contend that the general public is not well informed about their rights under the Privacy Rule. According to these organizations, patients may not understand the privacy notices they receive, or they do not focus their attention on privacy issues when the notices are presented to them. Some evidence of patients' lack of understanding is reflected in the 5,648 complaints filed with OCR in the first year most entities were required to be compliant with the Privacy Rule. Of the roughly 2,700 complaint cases OCR closed from April 14, 2003, through April 13, 2004, nearly two-thirds were found not to fall within the scope of the Privacy Rule because they either involved accusations of actions that were not prohibited by the regulation, involved entities that were not "covered entities" as defined by the Privacy Rule, or involved actions that occurred before covered entities were required to be compliant. Of those cases that were germane to the rule, OCR determined that half represented cases in which no violation had occurred.

We recommend that the Secretary of HHS modify the Privacy Rule to require that privacy notices state that patient information will be disclosed to public health authorities when required by law, and to exempt such public health disclosures from the accounting-for-disclosures provision. We also recommend that the Secretary undertake a public information campaign to improve patients' awareness of their rights under the Privacy Rule.

In written comments on a draft of this report, HHS stated that our finding that implementation went more smoothly than expected during the first year is generally consistent with what the agency has heard from covered entities and others. Regarding our recommendation that mandatory reporting of health information to public health authorities be exempted from the accounting for disclosure requirement, HHS noted that it has considered such a change in the past and continues to monitor the need to modify the rule. However, we remain concerned that given the burden of accounting for mandatory disclosures to public health authorities, covered entities may be disinclined to add to their tracking requirements by responding to public health agencies' requests for voluntary reporting.

Regarding the recommendation for a public information campaign, HHS agreed that notices of privacy practices may appear too long and complicated and that consumers may not be closely reading their notices. HHS cited two new consumer fact sheets posted to its Web site on August 17, 2004, a toll-free call-in line to respond to questions about the rule, and efforts to encourage covered entities to develop consumer-friendly notices that highlight key information. We believe it is important that, in current and future efforts to educate the public, HHS more effectively disseminate information about protections provided under the Privacy Rule.

Background

The Privacy Rule addresses the use and disclosure of individuals' health information and establishes individuals' rights to obtain and control access to this information.[3] Specifically, the rule covers "protected health information," defined as individually identifiable health information that is transmitted or maintained in any form.[4] It applies to "covered entities," defined as health plans, health care clearinghouses, and health care providers that transmit information electronically with respect to certain transactions.[5] The protections under the Privacy Rule extend to all individuals, regardless of the state in which they live or work, but the rule does not preempt state privacy laws that are more stringent—that is, more protective of health information privacy.

[3] 45 C.F.R. pts. 160 and 164 (2003).

[4] "Health information" includes oral or written information created or received by health care providers or others related to the medical condition of, providing health care to, or paying for health care provided to an individual. "Individually identifiable health information" is health information that identifies an individual or from which there is a reasonable basis to believe an individual may be identified.

[5] Providers include hospitals, physicians, dentists, pharmacies, and any other persons or organizations that furnish, bill, or are paid for health care. "Health plans" refers to individual and group plans that provide or pay the cost of medical care. "Clearinghouses" refers to entities that facilitate the flow of information between providers and payers. In addition, sponsors of Medicare-endorsed prescription drug discount cards were added as covered entities by the Medicare Prescription Drug, Improvement, and Modernization Act of 2003, although the Secretary is authorized to waive portions of the privacy rule to promote sponsor participation.

Permissible Uses and Disclosures

Under the Privacy Rule, a covered entity may use and disclose an individual's protected health information without obtaining the individual's authorization when the information is used for treatment, payment, or health care operations. Protected health information may also be disclosed without an individual's authorization for such purposes as certain public health and law enforcement activities, and judicial and administrative proceedings, provided certain conditions are met. In addition, an individual's authorization is not required for disclosures for research purposes if a waiver of authorization, under defined criteria, is obtained from an institutional review board (IRB) or a privacy board.[6]

Except where the rule specifically allows or requires a use or disclosure without an authorization, the individual's written authorization must be obtained; for example, authorization is generally required for disclosures to life insurers or employers. In addition, the rule contains specific provisions that generally require an individual's authorization for the use or disclosure of psychotherapy notes or of protected health information for marketing purposes.

In many circumstances, a provider or health plan can choose not to disclose information, regardless of whether an individual's authorization is required. The Privacy Rule allows covered entities to use their discretion in deciding whether to disclose protected health information for many types of disclosures, such as those to family and friends, public health authorities, and health researchers.

Individual Privacy Rights

The Privacy Rule provides individuals with a number of rights regarding access to, and use of, their health information. Specifically, the rule provides the following:

- *Access to and amendment of health information.* Individuals have the right to inspect and copy their protected health information and to request amendments of their records.

[6] An IRB is a board, committee, or other group established in accordance with applicable federal regulations and formally designated by an institution to review human subject research. A privacy board is a review body that may be established to act on research requests under the Privacy Rule in place of using an IRB. Before issuing waivers, these boards must determine, among other things, that the use or disclosure of protected health information involves no more than a minimal risk to the privacy of the individuals.

- *Notice of privacy practices*. Individuals generally have a right to written notice of the uses and disclosures of their health information that may be made by a covered entity as well as the individual's rights and the entity's duties with respect to that information.

- *Accounting for disclosures*. Individuals generally have the right to request and receive a listing of disclosures of their protected health information that is shared with others for purposes other than treatment, payment, or health care operations.

- *Complaints*. In addition to being able to complain directly to a covered entity, any person who believes a health care provider, health plan, or clearinghouse is not complying with the Privacy Rule may file a complaint with the Secretary of HHS.[7]

Responsibilities of Health Care Providers, Health Plans, and Clearinghouses

Covered entities are required to comply with Privacy Rule provisions and follow various procedures. They must do the following:

- *Develop policies and procedures for protecting health information.* A covered entity must maintain administrative, technical, and physical safeguards. Among other requirements, a covered entity must also designate a privacy official, train its employees on the entity's privacy policies, and develop procedures to receive and address complaints.

- *Limit information used and disclosed to the minimum necessary.* Covered entities must make reasonable efforts to limit their employees' access to identifiable health information to the minimum needed to do their jobs. When sharing protected health information with other entities (such as collection agencies and researchers), they must make reasonable efforts to limit the information disclosed to the minimum necessary to accomplish the purpose of the data request. However, providers may share the full medical record when the disclosure is for treatment purposes.

- *Account for disclosures of protected health information.* Upon request, covered entities must provide individuals with an accounting of disclosures of their protected health information made in the preceding

[7] The Privacy Rule does not create a private cause of action—that is, a federal right to sue for violations of the rule.

6 years. This requirement applies to most disclosures other than those for treatment, payment, or operations purposes, including those that are mandated by law—such as certain disclosures to public health entities and law enforcement agencies. The accounting must include the date of each disclosure; the name and, if known, the address of the entity or person who received the information; a description of the information disclosed; and a statement of the purpose of the disclosure.

- *Ensure that "downstream users" protect the privacy of health information by implementing business associate agreements.* Covered entities must enter into a contract or other written agreement with any business associates with which they share protected health information for various purposes. A business associate performs certain functions or activities—such as claims processing and benefit management—on behalf of a covered entity involving the use or disclosure of individually identifiable health information. Business associate contracts must establish conditions and safeguards for uses and disclosures of identifiable health information and authorize termination of contracts if the covered entities determine that business associates have violated the agreements.

Disclosures to Researchers Seeking Health Information from Covered Entities

The regulation establishes requirements that apply to both federally and privately funded research that seeks to use protected health information:

- Researchers may seek to obtain from covered entities health information without authorization if the data do not identify an individual and there is no reasonable basis to believe it could be used to identify an individual.[8]

- Researchers must use one of three options to gain access to protected health information: obtain patient authorization, obtain a waiver of authorization by having their research protocol reviewed and approved

[8] "De-identified" information is not considered individually identifiable health information. De-identification of data can be achieved in two ways: (1) all individually identifiable data—for example, names, addresses, phone numbers, Social Security numbers, dates indicative of age, and other unique identifiers—are removed or (2) a qualified statistician, using generally accepted statistical and scientific principles, determines that the risk is very small that the individual could be identified.

by an IRB or privacy board, or use a limited data set provided by the covered entity.[9]

Responsibilities of HHS's Office for Civil Rights

OCR has responsibility for implementing and enforcing the Privacy Rule as follows:

- *Provide guidance.* OCR is responsible for communicating policies contained in the Privacy Rule by issuing guidance to answer common questions and clarify certain provisions. Mechanisms by which OCR makes information available to various entities on its Web site include links to guidance documents as well as answers to frequently asked questions (FAQ). In addition, OCR has provided guidance through roundtable discussions, answers to written inquiries, an automated e-mail notification system, a toll-free hotline for questions about the Privacy Rule, as well as presentations and telephone conference calls.

- *Administer a complaint process.* OCR is responsible for investigating complaints received from health care consumers.

- *Enforce compliance.* OCR may provide covered entities with technical assistance to help them comply voluntarily with the Privacy Rule. OCR investigates complaints and may conduct reviews to determine if covered entities are in compliance and attempts to resolve issues of noncompliance through informal means. Violators are subject to civil and criminal penalties.[10] OCR administers the civil monetary penalties while the Department of Justice administers criminal penalties involving a knowing disclosure or obtaining identifiable health information in violation of HIPAA.

[9] A limited data set has many direct identifiers removed, such as name, street address, telephone number, and Social Security number.

[10] Civil monetary penalties can include fines of $100 per violation up to $25,000 per year for all violations of an identical requirement. Criminal penalties can include fines of up to $250,000 and imprisonment for up to 10 years.

Compliance Difficulties for Providers and Health Plans Have Eased, but Problems Remain

Organizations representing providers and health plans stated that implementation of the Privacy Rule was smoother than expected over the past year and that some initial confusion has abated. Although many provider and health plan organizations reported dealing with various ongoing problems, they noted that two provisions were particularly burdensome: the requirement to maintain a record of certain disclosures of patient information and the requirement to create business associate agreements with downstream users of protected health information. Several organizations suggested that OCR could take steps to facilitate compliance with these provisions.

Confusion among Providers and Health Plans Has Diminished

Some organizations we interviewed told us that the first year they were required to be compliant with the Privacy Rule was smoother than they had anticipated. The American Medical Association and the American Hospital Association stated that in general, they have heard relatively few negative reactions from their members during the past year. Many provisions were considered straightforward and relatively easy to implement, including developing the notice of privacy practices and limiting disclosures for marketing purposes. In addition, many provider, health plan, and consumer representatives reported that the Privacy Rule has increased provider awareness of, and sensitivity to, patient privacy issues, and new privacy procedures have become routine practice. For example, representatives from the American Health Information Management Association (AHIMA)—which assists providers with their management of protected health information—noted that the Privacy Rule has helped to make staff working for covered entities more aware of the flow of patient information.

Organizations we interviewed also reported that some early confusion has subsided. Groups commented that initial confusion stemmed from challenges in understanding and implementing the Privacy Rule. The American Hospital Association, for example, stated that hospitals were initially concerned about the requirement to limit information disclosures to the "minimum necessary" but now understand that they can share the information needed to ensure that appropriate clinical care is provided to their patients. Representatives from the American Pharmacists' Association (APhA) stated that members faced initial confusion implementing the Privacy Rule, but that pharmacies have since developed new standard procedures to address these issues. Representatives of the American Medical Association noted that after receiving and resolving

many calls requesting clarification early in the year, it has since received few calls from its members related to the Privacy Rule.

However, organizations also commented that some uncertainties and misunderstandings continue. For example, provider groups stated that some physicians and hospitals remain unclear about what type of information may be disclosed for law enforcement purposes. In addition, health plan representatives reported ongoing difficulties associated with knowing whether state laws prevail over the Privacy Rule. Despite these problems, AHIMA representatives told us that "the number of people talking about the ship sinking" because of the Privacy Rule has decreased.

Overall, the organizations had mixed opinions about the extent to which OCR's guidance facilitated implementation of the Privacy Rule. As of June 29, 2004, OCR has posted 223 FAQs and answers on its Web site. While some provider and health plan representatives reported that the OCR Web site—particularly the FAQs—was very helpful, others stated that the FAQs were not specific enough to explain certain vague or ambiguous Privacy Rule provisions. Furthermore, organizations we interviewed stated that various types of guidance offered by OCR—including roundtable discussions and guidance on particular provisions—would have been more helpful if they had been offered sooner. For example, representatives from the American Health Care Association (AHCA) stated that if they had received clarification and guidance from OCR earlier, they would have had fewer problems implementing the rule.

Two Provisions Were Commonly Cited as Particularly Difficult to Implement

Although provider and health plan representatives reported dealing with a variety of ongoing problems, we consistently heard from them that two provisions were especially burdensome. These were the provisions that require accounting for disclosures and business associate agreements.

Accounting for Disclosures

Most provider and health plan organizations we interviewed identified the requirement to account for certain disclosures as unnecessarily burdensome. These organizations reported that significant time and resources are needed to establish and maintain systems to track disclosures. For example, in hospitals, various departments keep patient information in separate systems that are not necessarily electronically linked. According to the Health Care Compliance Association, hospitals have had to revise systems to establish electronic links or have had to create manual tracking mechanisms. Similarly, representatives from

America's Health Insurance Plans (AHIP) reported that many health plans or insurers generally keep information related to one patient in multiple systems—for example, separate systems for enrollment, claims payment, and customer service—making it difficult to track all information disclosures for that patient.

In addition to difficulties experienced when tracking disclosures of protected health information, provider and health plan representatives also expressed concern about the volume of disclosures that must be tracked. They commented that frequent, diverse disclosures required by law add significantly to the volume of information that must be continually tracked. These include disclosures to public entities to maintain disease registries, vital statistics, and other health databases.[11] For example, the Minnesota Department of Public Health identified over 50 state statutes in which health information may or must be released to specific state or local organizations, such as health departments, health licensing boards, and schools. Blue Cross Blue Shield Association (BCBSA) representatives told us that accounting for the disclosures of births and deaths to state health departments—required by state law—can be burdensome. They noted that some state laws require health plans to report information to the health department quarterly, while others require reporting information monthly. One organization we spoke with indicated that its members expect that complying with the provision to account for disclosures will become increasingly difficult, because they need to track these disclosures for 6 years to meet obligations under the Privacy Rule.

Moreover, many organizations we interviewed questioned whether the Privacy Rule's accounting provision generates much benefit for patients. These organizations reported that their members have received few or no requests from patients for an accounting of the disclosures of their protected health information. To somewhat reduce the burden of the requirement to account for disclosures, several organizations suggested that OCR modify the rule to require covered entities to inform patients in the privacy practices notice that when required by law, their information will be disclosed to public health organizations and law enforcement agencies. This modification would inform patients of disclosures required

[11] Examples of the types of health information providers are asked to report included births and deaths, cancer cases, brain and spinal cord injuries, child immunizations, blood lead analyses, and reports of work-related injuries.

by law and would obviate the need to track these disclosures as they occur.[12]

Business Associate Agreements

Provider and health plan representatives reported that significant resources have been required to implement business associate agreements. These organizations commented that some of the burden associated with implementing this provision has stemmed from confusion and variation in determining which relationships with downstream entities require business associate agreements.[13] The Medical Group Management Association (MGMA) stated that there is still uncertainty among its members and that it receives calls weekly about business associate agreements. APhA representatives attributed pharmacists' difficulties determining which entities were business associates to the provision's broad language and lack of adequate OCR guidance.

Although the Privacy Rule provided for phased-in implementation of business associate agreement requirements to accommodate existing contracts, provider and health plan groups viewed the business associate agreements provision as very burdensome.[14] Organizations we interviewed stated that some of their members have spent substantial amounts of time and money to develop thousands of business associate agreements with downstream users of protected health information, though they did not estimate specific amounts. Provider and health plan representatives reported that high costs have been associated with the need for legal counsel to negotiate and customize agreements with the multiple and various business associates. For example, BCBSA officials stated that some of their business associates have requested specific and sometimes "excessive" details in their agreements. They noted that business

[12] In August 2002, HHS determined that elimination of this requirement was not justified without ensuring the individual's knowledge of such disclosures.

[13] The Joint Commission on Accreditation of Healthcare Organizations and the National Committee for Quality Assurance recently established a certification program—called the Privacy Certification for Business Associates program—that is intended to provide business associates with independent verification that they are complying with the Privacy Rule. Both of these organizations assess providers' compliance with quality standards.

[14] Covered entities with existing written contracts or agreements with business associates prior to October 15, 2002, that were not renewed or modified prior to April 14, 2003, were permitted to continue to operate under those contracts until they renewed them or until April 14, 2004, whichever came first.

associates sometimes regard the agreements as an opportunity to include new provisions in their contracts that are unrelated to health privacy.

The Joint Commission on Accreditation of Healthcare Organizations (JCAHO), however, was able to successfully avoid these types of problems by including a standard business associate agreement as an addendum to applications for health care accreditation. As a result, it has had "excellent compliance and cooperation from accredited entities," according to JCAHO representatives. In contrast, hospitals and other providers negotiating individually with business associates do not have similar leverage to compel the use of their particular agreements.

Some organizations representing providers and health plans suggested that OCR provide more guidance to covered entities about when and how to enter into a business associate agreement. These organizations did not consider OCR's existing guidance specific enough to assist providers and health plans with their agreements.[15] APhA representatives stated that OCR's guidance on business associate agreements has "led to more questions."

Constraints on Access to Data Have Raised Concerns for Public Health Entities, Researchers, and Patient Advocates

Organizations representing public health agencies, research entities, and patient advocates identified several areas in which efforts to apply the Privacy Rule have created new challenges. State and federal agencies reported having to take explicit action—including outreach efforts and changes in state law—to ensure that providers and health plans continue to report health information for public health activities. Researchers pointed to increased difficulty in obtaining patient data to conduct clinical or health services research. Patient advocates also identified obstacles in obtaining protected health information from providers and plans on behalf of their clients. Many of these challenges have been attributed to misunderstandings or confusion about how to interpret the rule in conjunction with other federal requirements. Most organizations found providers reluctant to share information without patient authorization when the rule permitted providers such discretion. The burden of accounting for disclosures and liability concerns were two reasons often cited for their reluctance.

[15] OCR posted on its Web Site a fact sheet and FAQs as guidance for the business associate provisions in July 2001, and sample contract language in August 2002. OCR updated the fact sheet and the FAQs for the business associate provisions in December 2002.

State and Federal Agencies Have Had to Increase Efforts to Obtain Data for Public Health Monitoring

Organizations representing state public health officials told us that the Privacy Rule has hindered access to patient health information because some providers are reluctant to report to public health authorities. They experienced this difficulty despite the fact that under the Privacy Rule, providers and health plans may report to public health authorities without a patient's authorization.[16] This provision applies both where a law requires that certain health information—such as immunizations—be reported and where a public health agency requests that providers voluntarily report certain information.

Public health organizations—such as the Council of State and Territorial Epidemiologists (CSTE) and CDC—reported several cases where obtaining patient health information has become more difficult. For example, a CSTE survey of 40 state and local programs designed to detect early signs of an epidemic found that 3 programs experienced "substantial" problems and 10 experienced "some" problems with obtaining health information from providers because of patient confidentiality concerns.[17] In another example, a CDC representative reported facing obstacles to its surveillance of mental health disabilities. CDC's efforts to collect data on individuals with certain mental health diagnoses met resistance from a large clinic and an inpatient mental health facility. As a result, CDC redesigned its study and had to approach different providers to participate in its data collection effort.

Public health organizations attributed the difficulty in obtaining public health data from providers and plans to several factors. First, organizations we spoke with believed that providers have a disincentive to report data requested by public health agencies because of the provision to account for such disclosures. According to a state public health agency representative, the necessary tracking of disclosures has had a major impact on the state's public health activities. This is consistent with concerns expressed by representatives of health plans, physicians, hospitals, and long-term care facilities about the burden of accounting for certain disclosures. Second, some providers were confused about the rule in that they believed they were permitted to report to public health

[16] While patient authorization is not required for disclosures for public health purposes, providers and health plans must maintain an accounting for such disclosures under the Privacy Rule.

[17] The survey response rate was 74 percent (29 of 40 programs).

agencies only when specifically required by federal or state law. A representative of CDC noted that in some states that did not mandate reporting of birth defect surveillance data, providers were initially unwilling to disclose this information. Third, state officials noted that providers are concerned legal action might be taken against them if they provide health information to public agencies. In CDC's efforts to monitor mental health disabilities, a provider cited fear of liability associated with improper disclosure of protected health information as the reason it declined to participate.

The organizations we interviewed also reported that state and federal health agencies have taken various actions to facilitate public health reporting. These include changes in state law, enhancements to the data collection process, and targeted Privacy Rule education. For example,

- Kentucky, Massachusetts, and North Dakota revised regulations and laws to clarify the circumstances for reporting to public health agencies without patient authorization, to make state law more consistent with the Privacy Rule, and to make certain public health reporting mandatory.

- CDC modified its survey procedures for a group of health care provider surveys, known as the National Health Care Survey, to help providers participate in the surveys under the Privacy Rule. The modifications included creating a document that providers can use to account for disclosures.

- The Minnesota Department of Health developed a series of fact sheets that clarify, for each of several different types of disease reporting, the specific authority in the Privacy Rule that allows reporting of data to the department without patient authorization.

Like the health plan and provider groups, organizations representing public health agencies stated their desire that the Privacy Rule be amended to exempt reporting to public health agencies from the accounting provision and announce in the privacy practices notice that this information will be disclosed as required by law. They contended that this approach would significantly reduce burden and remove the incentive that exists for providers to avoid disclosure of protected health data to public health agencies.

Research Groups Report Unnecessary Delays and Less Access to Health Data

Organizations representing health services and clinical researchers, such as Academy Health, the Association of American Medical Colleges, the Association of Clinical Research Organizations, and the National Cancer Advisory Board, reported that access to data for research has been delayed due to the varying approaches that some providers are taking to research requests under the Privacy Rule. They reported that research studies involving several sites of care have been delayed because of the different confidentiality requirements at study provider sites. Under the rule, researchers must obtain IRB or privacy board approval for their studies to waive the patient authorization requirement. HHS guidance states that a multisite research study need obtain approval from only one of the provider sites, but researchers' organizations contend that often each provider institution requires that its IRB approve the waiver request. They noted that meeting the requirements of multiple IRB reviews can add substantial time to completing these studies.

Under the Privacy Rule, researchers seeking authorization to use patient information must pursue their requests through the patients' providers. Organizations reported that smaller providers with more limited administrative resources—such as some group practices and rural community hospitals—are reluctant to facilitate research studies because of misunderstanding of the rule and the added burden of contacting patients. Providers may also decline to participate because of concern about liability and because of the administrative burden of the accounting for disclosures requirement. For example, the Association of American Medical Colleges reported that some physicians no longer contribute data to research registries for cancer because of the additional resources required to track these disclosures.

Another issue raised by several organizations we spoke with concerned the perceived conflicts between the Privacy Rule and federal regulation governing the protection of human subjects in research, known as the Common Rule. Research groups noted that differences between Privacy Rule and Common Rule requirements may cause confusion among researchers and covered entities and create unnecessary obstacles to research. For example, they stated that one difference relates to the scope of authority of informed consent or authorization: informed consent by patients under the Common Rule covers the research effort as a whole, including future disclosures from registry and data depositories. In contrast, they noted that a patient's authorization or an IRB's waiver of authorization covers only a specific research study and not future unspecified research under the Privacy Rule. Some national organizations

expressed concern that providers and health plans may find it too confusing to comply with both the Privacy Rule and Common Rule requirements in responding to research proposals and requests. An AHIMA official reported that in some cases, providers and health plans "just threw up their hands and said they would just not give information to researchers."

CMS—a source of health services utilization data on Medicare beneficiaries—did not approve research requests for approximately 6 months while it developed new criteria and procedures for review of research requests to comply with the Privacy Rule. CMS now requires that researchers, who submit about 1,000 requests each year, provide more information about their study methodology and demonstrate that their research purpose is consistent with CMS's mission. To comply with the Privacy Rule, CMS established a privacy board to review research requests. The board meets once a month, which lengthens this phase of CMS's research approval process.

The Association of American Medical Colleges, the Association of Clinical Research Organizations, and public health organizations such as the Association of State and Territorial Health Officials and CSTE reported that OCR's guidance has not addressed some of the key misunderstandings and fundamental problems associated with the Privacy Rule's impact on research. Ambiguity remains in determining whether a health survey activity is considered health care operations or research and whether a public health entity's data request is part of its public health activities or is for research. These organizations stated their desire for OCR to address concerns through official revisions to the rule and issuance of federal guidance. They believe that compared with OCR's efforts to provide information on its Web site, such official actions would "carry more weight" among providers, health plans, and research organizations.

Patient Advocates Report Obstacles to Obtaining Data on Behalf of Patients

Organizations representing patient advocates reported that their members face new obstacles when seeking access to protected health information on behalf of patients. Such access problems, they say, are due to excessive paperwork, misunderstanding of the rule, and reluctance by providers and health plans to share information with legal aid attorneys, state ombudsmen, and others when the rule permits discretion. The rule gives providers and plans some latitude in exercising their professional judgment about when to disclose protected health information to individuals serving as patient advocates who are not "personal representatives" as defined by

the Privacy Rule.[18] Factors such as liability concerns and the burden of accounting for disclosures may contribute to their guarded disclosure practices.

Representatives for Families USA's Health Assistance Partnership and the National Health Law Program reported problems when lawyers or other patient advocates sought a client's medical records. These organizations contend that some providers deny access and other providers delay or restrict access by requiring the use of a provider's customized authorization form. They asserted that it can be cumbersome if a patient's signature on multiple unique forms needs to be obtained from each provider. These organizations also noted that state ombudsmen services—telephonic programs that assist consumers, such as the elderly and disabled, with problems accessing health care—have had problems intervening on behalf of consumers over the telephone. Even after a consumer has given verbal approval, providers have declined to share information with the ombudsman in subsequent phone calls if the patient is not also on the telephone.

In addition, AHIP, AHCA, and BCBSA reported that families and friends of patients continue to face problems obtaining information to assist in patients' care. BCBSA reported that some plans are confused about how to implement the Privacy Rule's provisions for releasing information to families, friends, and others. Where the rule permits discretion, some covered entities have taken a strict approach to patient authorization requirements, requiring any adult calling on behalf of another adult to obtain an authorization form signed by the patient. For example, this approach resulted in one health plan requiring 10,000 patient authorizations during the first year.

Similarly, AHCA found that some long-term care facilities have taken a strict approach to disclosing information and do not provide information to nursing home residents' family members without patient authorization. AHCA also reported that the Privacy Rule does not address a potential conflict with the Omnibus Budget Reconciliation Act of 1987 that requires nursing homes to notify families of incidents or significant changes in health status unless the resident exercises the right to privacy. Under the

[18] Under the Privacy Rule, a personal representative generally is a person who is lawfully authorized to act on behalf of the patient in making decisions related to health care.

Privacy Rule, a provider may, in certain situations, determine whether or not to share information with family based on professional judgment.

Evidence Suggests Patients Are Not Aware of Privacy Rights or May Misunderstand the Privacy Rule

Numerous organizations reported that patients are not aware of their rights under the Privacy Rule, either because they do not understand the notice of privacy practices, or because they have not focused their attention on privacy issues when the notices are presented to them. In the first year after entities were required to be compliant with the Privacy Rule, OCR received over 5,600 privacy complaints and closed about half of the complaint cases filed. Nearly two-thirds of the closed cases were resolved on the basis that they were outside the scope of the Privacy Rule, suggesting that patients may misunderstand their rights.

Diverse Groups Contend That Patients Are Not Well Informed of Their Rights

Consumer groups—including AARP, the Bazelon Center for Mental Health Law, the Health Privacy Project, the Health Assistance Partnership, and the National Health Law Program—reported that many patients are not aware of their privacy rights. They attribute this, in part, to the use of customized privacy notices. For example, consumer groups reported that typical privacy notices, as drafted by providers and health plans, are often difficult to read and understand. The Health Privacy Project maintained that the privacy notices are written primarily to protect providers and health plans from enforcement actions, rather than as a vehicle to inform the patient. It noted that even basic information about disclosures and the right to access records is often buried in the document.

Representatives of providers and health plans also stated that patients are largely unaware of their rights. According to AHIMA, patients are unaware of their privacy rights because the privacy notice is treated as one more piece of paper that they have to sign when they seek care. MGMA noted that some physicians have placed boxes in their offices specifically for the purpose of recycling the notices after patients discard them.

Representatives from both provider and consumer groups noted that the public should receive more education about how their rights have changed. MGMA told us that OCR has placed the burden of patient education on private organizations—such as professional associations, providers, and health plans—and that some of these organizations interpret the rule incorrectly. Moreover, provider and consumer groups stated that further OCR attention is needed to address the issue of privacy notices that are

difficult for patients to read and understand. Some groups told us that the notice of privacy practices could be made easier to comprehend by highlighting some key patient rights under the Privacy Rule.

Complaints Filed with HHS OCR Indicate That Patients May Misunderstand the Privacy Rule

In the first year that entities were required to be compliant with the Privacy Rule, consumers and others filed 5,648 privacy-related complaints with OCR. The number of complaints received increased steadily from quarter to quarter, with each quarter's intake totaling 1,068, 1,392, 1,521, and 1,667, respectively. Overall, roughly half of the complaints filed in the rule's first year were closed as of early May 2004.

The database that OCR maintains on these complaints includes information that classifies one or more privacy issues raised in several broad categories. Data on the open and closed cases showed that the most commonly cited category (56 percent of complaints) was "impermissible uses and disclosures."[19] According to an OCR official, this could include allegations regarding patient billing information sent to the wrong address or FAX number, patient information seen or overheard in a doctor's office or hospital, or provider employees accessing patient information for their own personal or business benefit.[20] Approximately a third of the complaints cited inadequate safeguards for patient information, and 17 percent reported problems with patients gaining access to their own health information.

Patients have filed privacy complaints against many different types of health care entities. The two most commonly cited were private practices—comprising physicians, dentists, chiropractors, and similar licensed health professionals—and hospitals—including general, psychiatric, and specialty hospitals. Together, private practices and

[19] The percentages provided on cited categories reflect complaints for which this information was recorded. The OCR complaint data lacked such information for 40 percent of open cases and 46 percent of closed.

[20] OCR defines "impermissible uses and disclosures" as any use or disclosure of protected privacy information without patient authorization that falls outside of the permitted uses specified in the regulation. The OCR database provides no additional information describing the action or policy that prompted these complaints.

hospitals accounted for 41 percent of privacy complaints with information on entity type recorded.[21]

For closed cases, the OCR database provides additional information, primarily related to the final disposition of the complaint. The majority of these complaints—79.1 percent—were not germane to the Privacy Rule, lacked sufficient information to process them, or fell into diverse miscellaneous categories. That left 20.9 percent of the closed privacy complaints that OCR concluded fell within the scope of the Privacy Rule (see table 1).[22]

Table 1: Outcomes of Privacy Complaints Closed by OCR from April 14, 2003, through April 13, 2004

Outcome category	Number of cases	Percentage
Germane to the Privacy Rule	*573*	*20.9*
Violation occurred and corrective action agreed to[a]	258	9.4
No violation occurred	315	11.5
Not germane to the Privacy Rule	*1,760*	*64.2*
Alleged action not prohibited by Privacy Rule	971	35.4
Entity cited in the allegation is not a covered entity	484	17.7
Alleged action took place before April 14, 2003, the compliance date of the Privacy Rule	264	9.6
Other	41	1.5
Indeterminate	*408*	*14.9*
Complaint incomplete	364	13.3
Miscellaneous and other	44	1.6
Total	**2,741**	**100.0**

Source: GAO analysis of OCR data.

[a]In these cases, OCR obtained voluntary compliance from covered entities and did not issue a formal violation finding.

About half of the germane complaints (representing 9.4 percent of total closed cases) involved a violation of the Privacy Rule substantiated by

[21] Many more open complaints (45 percent) than closed ones (4.5 percent) lacked information on entity type.

[22] There were no complaints with missing data with respect to case closure disposition.

OCR's investigation where the provider or plan agreed to correct its policies or procedures. For the rest of these germane complaints (11.5 percent of total closed cases), OCR determined that no violation had occurred. By May 2004, OCR had not recommended sanctions against any provider or health plan for privacy violations, but this remained a potential outcome for the first-year complaints that were still open at that point.

Nearly two-thirds of the privacy complaints closed during the rule's first year of operation fell outside the scope or time frame of the rule. This included the 35.4 percent of closed privacy complaints that involved alleged actions by providers, health plans, or other entities that OCR determined would not constitute violations of the regulation even if true. In other words, they concerned actions to which the patient might object, but that were not prohibited by the Privacy Rule. An additional 17.7 percent of closed complaints involved entities that were not "covered entities" as defined by the Privacy Rule, and 9.6 percent cited actions that occurred before covered entities were required to be compliant. However, OCR officials stated that the proportion of complaints closed because they were not germane to the Privacy Rule may have been higher in the first year of the rule's implementation than it will be in later years because OCR can generally complete its processing of such complaints more quickly than complaints that require full-scale investigations. Just over half of the complaints received in the first year remained open in early May 2004.

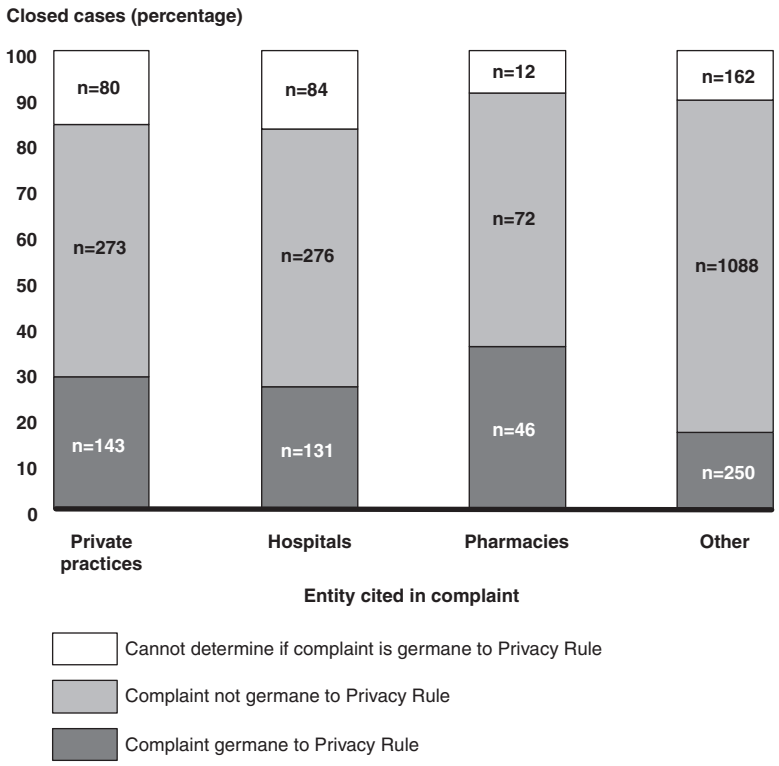
Finally, about 15 percent of closed complaints fell into one of a number of miscellaneous categories or, more commonly, could not be pursued because OCR did not receive, and could not obtain, critical information. For example, some complaints lack addresses or telephone numbers by which the persons filing the complaints could be contacted for more information.

Closed complaints involving three major categories of providers—private practices,[23] hospitals, and pharmacies—were more likely to be judged germane under the Privacy Rule by OCR than were complaints about other organizations. Nevertheless, for each of these major provider types, as well as for all other entities cited in privacy complaints, OCR found that a clear majority of the complaints it closed were not germane to the regulation because they either involved accusations of actions that were not

[23] Private practices include physicians, dentists, chiropractors, osteopaths, and other licensed medical providers.

prohibited by the regulation, involved entities that were not "covered entities" as defined by the Privacy Rule, or involved actions that occurred before covered entities were required to be compliant (see fig. 1).

Figure 1: Outcomes of Privacy Complaints Closed by OCR from April 14, 2003, through April 13, 2004, by Type of Entity Cited



Source: GAO analysis of OCR data.

Note: Numbers in columns represent the number of complaints for that outcome category.

The similarity of this pattern across different types of entities suggests that patients may misunderstand the scope of the protections provided to them under the Privacy Rule. The pattern is also consistent with consumer advocates' opinions concerning the limitations of privacy notices in informing patients about their rights under the Privacy Rule.

Conclusions

Overall, in its first year, HIPAA's Privacy Rule has resulted in both positive and negative experiences among covered entities and other users of health

information. Health care staff have been sensitized to privacy issues and the procedures required of their organizations to protect patient health information. Providers and health plans have taken steps to develop working environments that are sensitive to patient privacy and to enhance staff understanding of how to handle the complexities of complying with the Privacy Rule.

However, some operational issues and misconceptions about the rule continue to raise concerns. A prime example is the requirement to account for disclosures for public health purposes that are mandated by law. This requirement is seen by many to have created a costly and unnecessary demand on providers and health plans and a drag on the flow of information for purposes considered to be in the public interest.

Providers and health plans that are uncertain or misinformed about their privacy responsibilities have often responded with an overly guarded approach to disclosing information, resulting in procedures that may be more protective of the organizations than necessary to ensure compliance with the Privacy Rule. At the same time, the job of educating the public about the content and intent of the Privacy Rule has been relegated to providers and health plans and their privacy notices have not consistently provided a clear message to patients.

Recommendations for Executive Action

We recommend that to reduce unnecessary burden on covered entities and to improve the effectiveness of the Privacy Rule, the Secretary of HHS take the following two actions:

- Modify the Privacy Rule to (1) require that patients be informed in the notice of privacy practices that their information will be disclosed to public health authorities when required by law and (2) exempt such public health disclosures from the accounting-for-disclosures provision.

- Conduct a public information campaign to improve awareness of patients' rights under the Privacy Rule.

Agency Comments and Our Evaluation

In written comments on a draft of this report, HHS agreed with our finding that implementation went more smoothly than expected during the first year, confusion has diminished, and new privacy procedures have become routine practice for staff. They stated that the experience of providers and

health plans in implementing the Privacy Rule, as we reported, were generally consistent with what HHS has heard from many covered entities and others. (See app. II.)

Regarding our recommendation that mandatory reporting of health information to public health authorities be exempted from the accounting for disclosure requirement, HHS noted that it has considered such a change in the past and continues to monitor the need to modify the Privacy Rule. In August 2002, HHS considered exempting public health disclosures from the accounting provisions whether required by law or not, but decided against such a modification pending further experience with the rule. HHS acknowledged that covered entities continue to report difficulties tracking such disclosures and stated that its guidance documents emphasize flexibility in how covered entities structure their record keeping.

Given HHS's goal of ensuring effective patient privacy protections without imposing unnecessary costs or barriers to quality health care or interfering with other important public benefits, we remain concerned that the accounting for disclosure provision as applied to mandatory public health reporting may not support this goal. Effective privacy notices could be used to inform patients of public health disclosures required by law and, in turn, reduce the need to track these numerous disclosures. Furthermore, public health officials noted that the burden imposed by accounting for legally required disclosures may generate the unintended consequence of reducing the amount of information voluntarily reported to public health authorities. To the extent that covered entities are discouraged in this way, the public interest may be negatively affected.

In commenting on our second recommendation, to conduct a public information campaign to improve awareness of patient's rights under the Privacy Rule, HHS agreed that notices of privacy practices may appear too long and complicated and that consumers may not be closely reading their notices. HHS stated that the complaint data received by OCR may not indicate that consumers are unaware of their rights under the rule, but rather that they may not properly understand them. Regarding its consumer outreach, HHS pointed to two new consumer fact sheets posted to its Web site on August 17, 2004, a toll-free call-in line to respond to questions about the rule, and efforts to encourage covered entities to develop consumer-friendly notices that highlight key information.

Evidence from numerous organizations indicated that consumers are largely unaware of their rights under the Privacy Rule, and our analysis of

OCR complaint data suggested that consumers may misunderstand the scope of the protections provided. A more diverse approach to consumer outreach may be necessary to effectively communicate the new privacy rights. The information available on the HHS Web site and from the call-in line provide access to a portion of the general public but may not reach the many consumers who do not know of these sources. We believe it is important that, in current and future efforts to educate the public, HHS more effectively disseminate information about protections provided under the Privacy Rule.

As agreed with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days from its date. At that time, we will send copies of this report to the Secretary of HHS and to other interested parties. In addition, this report will be available at no charge on GAO's Web site at http://www.gao.gov. We will also make copies available to others upon request.

If you or your staff have any questions about this report, please call me at (312) 220-7600. Another contact and key contributors are listed in appendix II.

Sincerely yours,

Leslie G. Aronovitz
Director, Health Care—Program
Administration and Integrity Issues

Organizations Interviewed

We included the following national organizations and federal agencies in our review.

Health Care Providers	American Health Care Association American Hospital Association American Medical Association American Pharmacists' Association Medical Group Management Association National Association of Community Health Centers
Health Plans	America's Health Insurance Plans Blue Cross Blue Shield Association Medicare (HHS's Centers for Medicare & Medicaid Services)
Public Health	Association of State and Territorial Health Officials Council of State and Territorial Epidemiologists HHS's Centers for Disease Control and Prevention
Health Care Research	Academy Health Association of American Medical Colleges Association of Clinical Research Organizations National Cancer Advisory Board
Patient Advocates	AARP Bazelon Center for Mental Health Law Health Assistance Partnership Health Privacy Project National Health Law Program
Other	American Health Information Management Association Health Care Compliance Association Healthcare Leadership Council Joint Commission on Accreditation of Healthcare Organizations

Comments from the Department of Health and Human Services

DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of Inspector General

Washington, D.C. 20201

AUG 27 2004

Ms. Leslie G. Aronovitz
Director, Health Care—Program
Administration and Integrity Issues
United States Government Accountability Office
Washington, D.C. 20548

Dear Ms. Aronovitz:

Enclosed are the Department's comments on your draft report entitled, "Health Information: First-Year Experiences under the Federal Privacy Rule" (GAO-04-965). The comments represent the tentative position of the Department and are subject to reevaluation when the final version of this report is received.

The Department provided several technical comments directly to your staff.

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

Sincerely,

Lewis Morris
Chief Counsel to the Inspector General

Enclosure

The Office of Inspector General (OIG) is transmitting the Department's response to this draft report in our capacity as the Department's designated focal point and coordinator for Government Accountability Office reports. OIG has not conducted an independent assessment of these comments and therefore expresses no opinion on them.

COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO) DRAFT REPORT "HEALTH INFORMATION: FIRST-YEAR EXPERIENCES UNDER THE FEDERAL PRIVACY RULE" (GAO-04-965)

HHS appreciates the opportunity to comment on the GAO's draft report. The Department is committed to implementing strong and effective patient privacy protections that are appropriately balanced so as not to unnecessarily interfere with access to quality health care or other important public benefits and national priorities. The Privacy Rule affords health care consumers important new rights to access their health information and increases their ability to control uses and disclosures of this information.

The GAO draft report focuses on the experience of providers and health plans in implementation, and of researchers, public health entities, and patient advocates in obtaining access to health information during this first year of Privacy Rule compliance, as well as the extent to which patients appear to be aware of their rights. It is gratifying to hear from GAO's report that providers and health plan representatives reported that implementation of the Privacy Rule went more smoothly than expected during this first year, confusion has diminished, and that new privacy procedures have become routine practice for staff. This is consistent with what the Department itself has heard from many covered entities and other stakeholders.

The Department's Office for Civil Rights (OCR) is responsible for administering and enforcing the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. As part of that effort, OCR has undertaken expansive outreach to educate covered entities about the Rule, including providing guidance on an ongoing basis in targeted areas and to clarify aspects of the Rule as needed, and to educate the public about their new rights under the Rule. A significant number of guidance materials OCR has published, including materials published since GAO undertook this review, address areas GAO identifies as needing additional clarity.

OCR's ongoing outreach efforts include:

- Development and broad dissemination of guidance and other information on the OCR web site at http://www.hhs.gov/ocr/hipaa. The web site includes, among other materials,
    - a Summary of the Privacy Rule, with links to other helpful information on specific topics
    - fact sheets on general and specific topics of interest to various stakeholders, such as Business Associates, and most recently, a set of new Consumer fact sheets
    - hundreds of searchable answers to frequently asked questions, which have been accessed over 2.3 million times, including a newly-published FAQ on disclosures to law enforcement
    - sample business associate contract provisions
    - extensive guidance materials developed in conjunction with the National Institutes of Health and the Centers for Disease Control and Prevention that

1

explain the research and public health provisions of the Rule and
- information for consumers on how to file complaints with OCR

- Broadcasting to a listserv, which now has nearly 15,000 subscribers, to assist in making sure that guidance materials are broadly disseminated as soon as they are published.

- Offering a free call-in line for HIPAA Privacy Rule questions, 1-866-627-7748, in conjunction with the Centers for Medicare and Medicaid Services (CMS). Since April 2003, some 30,000 calls related to the Privacy Rule have been responded to.

- Giving hundreds of presentations and telephone audio conferences to varied audiences across the country on all aspects of the Privacy Rule.

OCR and the Department remain committed to these outreach and technical assistance efforts.

GAO Recommendation

Modify the Privacy Rule to (1) require that patients be informed in the notice of privacy practices that their information will be disclosed to public health authorities when required by law, and (2) exempt such public health disclosures from the accounting-for-disclosures provision.

HHS Response

The draft report and Recommendation reflect concerns we also have heard from certain covered entities and other stakeholders regarding the accounting for disclosures provision of the Privacy Rule. For example, we have heard concerns regarding the burden associated with accounting for routine public health disclosures, routine disclosures to Federal and State oversight authorities, and disclosures in other contexts, whether required by law or not. When modifying the Privacy Rule in August 2002 to address certain workability concerns, the Department considered the extent to which such disclosures should be exempted from the accounting provisions, seeking to balance an individual's right to know about disclosures of which he or she otherwise may not have specific knowledge, with the potential cost and other burdens on covered entities in providing the accounting. Ultimately, the Department decided against any such modification at the time, pending further experience with the Rule in this regard. Now, more than 1 year into implementation of the Privacy Rule, the Department continues to receive anecdotal accounts, such as are reflected in this GAO report, of challenges covered and entities faced in tracking disclosures that must be accounted for under the Rule, and that relatively few consumers have thus far requested an accounting.

The Department has responded to these concerns by publishing guidance that emphasizes that the Rule flexibly permits covered entities to structure their records systems in any way that efficiently permits them to comply with the Rule, and clarifying, for instance, that notations do not have to be made in each client file – particularly where more routine disclosures are

concerned and where the information can be retrieved, as needed, by other methods.

In addition, the Department continues to monitor experience with this aspect of the Rule, along with the benefits to consumers it affords, to determine whether modification of the Rule may be required. As with other areas of the Rule, our goal is to ensure that the Rule strikes the appropriate balance: affording individuals their rights, including the right to be informed of how their health information may be used and disclosed, without unnecessarily imposing costs or barriers to quality health care.

GAO Recommendation

Conduct a public information campaign to improve awareness of patients' rights under the Privacy Rule.

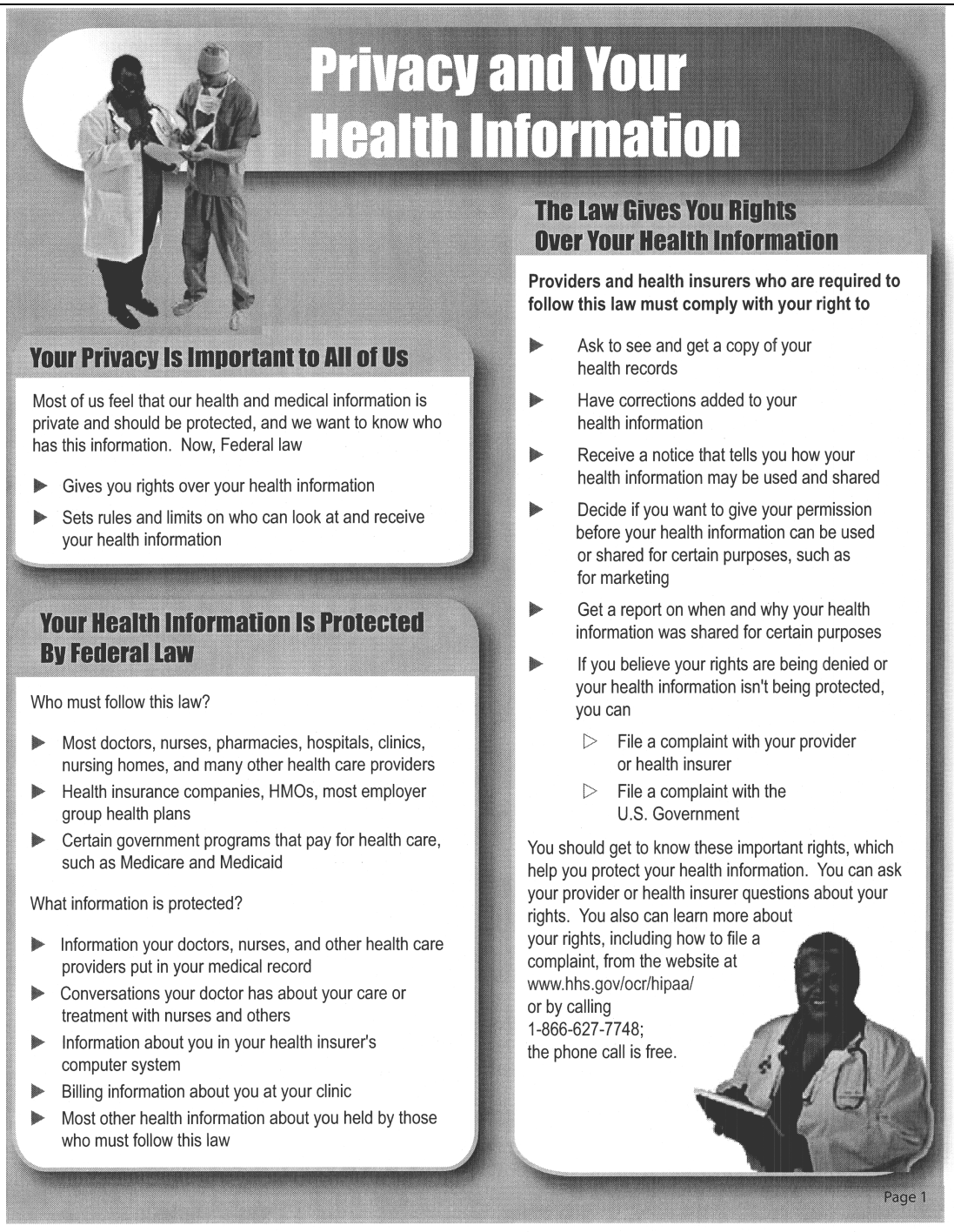
HHS Response

We fully agree it is essential that health care consumers are aware of their significant new rights under the Privacy Rule, and have been working diligently toward that end. For example, in recent weeks OCR published and is disseminating two new fact sheets (enclosed) – targeted specifically to consumers, and designed in a consumer-friendly format – that explain an individual's rights and protections under the Rule. As a further example, the toll-free call-in line continues to provide consumers and other callers with instant information about the Rule, and advises where additional information readily can be obtained.

We agree that many Notices of Privacy Practices may appear too long and complicated to consumers, and similarly are concerned with reports that consumers are not closely reading them. To address this, we have encouraged covered entities to focus on creating consumer friendly notices by using layered notices that describe the individual's rights and other key information in clear and simple language up front, and have required in the Rule itself that the notices be written in plain language. Further, the Privacy Rule requires covered health care providers with a direct treatment relationship with individuals to make a good faith effort to obtain a written acknowledgment of receipt of the notice, so that individuals are afforded an opportunity to focus on and discuss their privacy concerns and questions with their providers.

We note that the GAO-cited data on non-germane complaints may not actually indicate that consumers are unaware of their Privacy Rule rights, as GAO suggests. Rather, the number of such complaints could also indicate that consumers have been made aware, through the Notice of Privacy Practices and OCR's outreach efforts, of the important new rights they have with respect to their health information, though they may not comprehend entirely the parameters of those rights. For example, a consumer that has been made aware of the existence of protections now required under the Privacy Rule may file a complaint naming her provider even though that provider is not a covered entity; or the individual may believe that the Rule requires an action when it does not, as is the case, for instance, where a complainant alleges problems in having his medical records sent to his new doctor. In any case, OCR will continue its efforts to increase

consumer awareness about both the existence and nature of their rights and protections under the Rule.



Privacy and Your Health Information

Your Privacy Is Important to All of Us

Most of us feel that our health and medical information is private and should be protected, and we want to know who has this information. Now, Federal law

- Gives you rights over your health information
- Sets rules and limits on who can look at and receive your health information

Your Health Information Is Protected By Federal Law

Who must follow this law?

- Most doctors, nurses, pharmacies, hospitals, clinics, nursing homes, and many other health care providers
- Health insurance companies, HMOs, most employer group health plans
- Certain government programs that pay for health care, such as Medicare and Medicaid

What information is protected?

- Information your doctors, nurses, and other health care providers put in your medical record
- Conversations your doctor has about your care or treatment with nurses and others
- Information about you in your health insurer's computer system
- Billing information about you at your clinic
- Most other health information about you held by those who must follow this law

The Law Gives You Rights Over Your Health Information

Providers and health insurers who are required to follow this law must comply with your right to

- Ask to see and get a copy of your health records
- Have corrections added to your health information
- Receive a notice that tells you how your health information may be used and shared
- Decide if you want to give your permission before your health information can be used or shared for certain purposes, such as for marketing
- Get a report on when and why your health information was shared for certain purposes
- If you believe your rights are being denied or your health information isn't being protected, you can
  - File a complaint with your provider or health insurer
  - File a complaint with the U.S. Government

You should get to know these important rights, which help you protect your health information. You can ask your provider or health insurer questions about your rights. You also can learn more about your rights, including how to file a complaint, from the website at www.hhs.gov/ocr/hipaa/ or by calling 1-866-627-7748; the phone call is free.

Page 1

PRIVACY

The Law Sets Rules and Limits on Who Can Look At and Receive Your Information

To make sure that your information is protected in a way that does not interfere with your health care, your information can be used and shared

- For your treatment and care coordination
- To pay doctors and hospitals for your health care and help run their businesses
- With your family, relatives, friends or others you identify who are involved with your health care or your health care bills, unless you object
- To make sure doctors give good care and nursing homes are clean and safe
- To protect the public's health, such as by reporting when the flu is in your area
- To make required reports to the police, such as reporting gunshot wounds

Your health information cannot be used or shared without your written permission unless this law allows it. For example, without your authorization, your provider generally cannot

- Give your information to your employer
- Use or share your information for marketing or advertising purposes
- Share private notes about your mental health counseling sessions

For More Information

This is a brief summary of your rights and protections under the federal health information privacy law. You can learn more about health information privacy and your rights in a fact sheet called *"Your Health Information Privacy Rights"*. You can get this from the website at www.hhs.gov/ocr/hipaa/. You can also call 1-866-627-7748; the phone call is free.

Other privacy rights
Another law provides additional privacy protections to patients of alcohol and drug treatment programs. For more information, go to the website at www.samhsa.gov.

The Law Protects the Privacy of Your Health Information

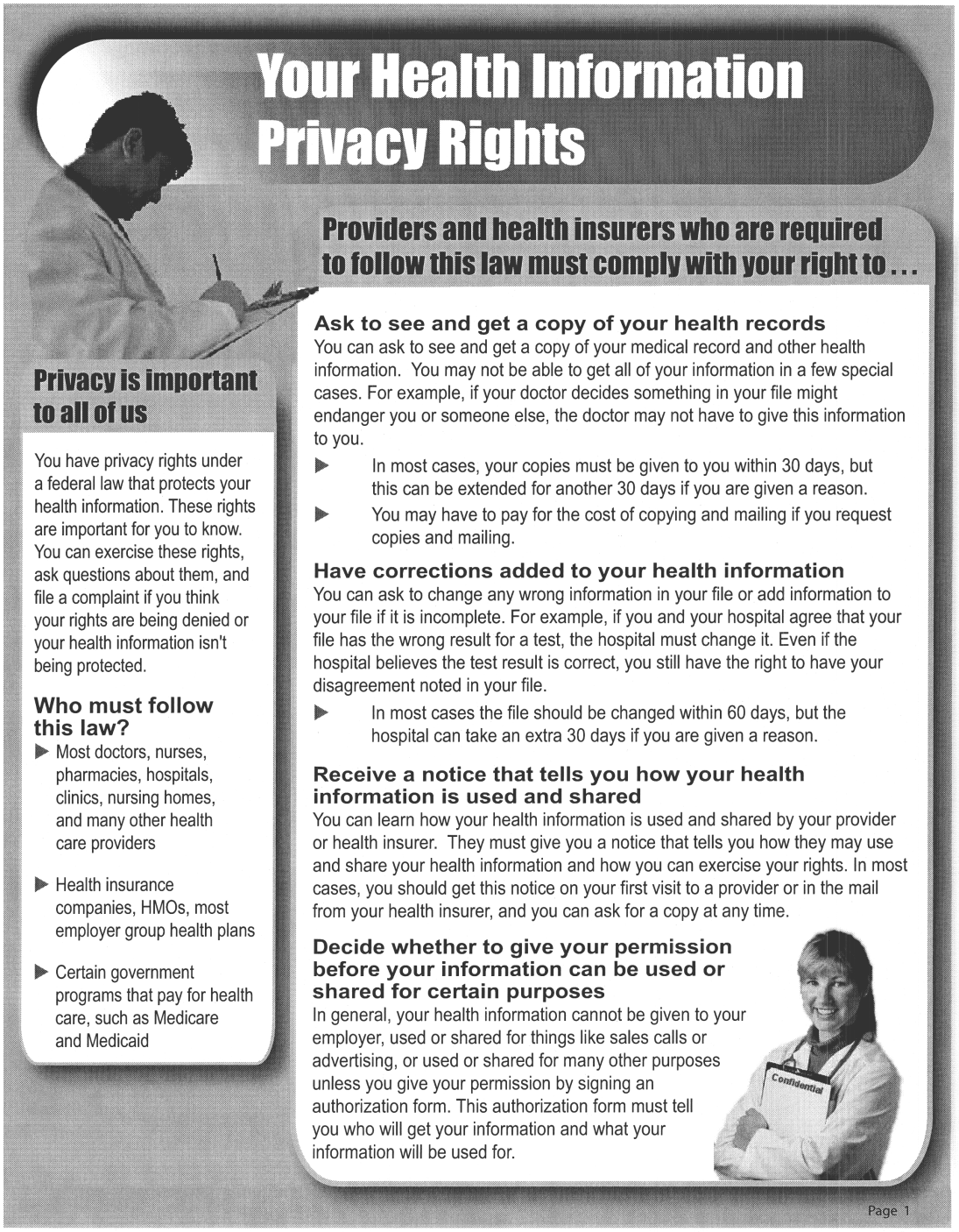
Providers and health insurers who are required to follow this law must keep your information private by

- Teaching the people who work for them how your information may and may not be used and shared
- Taking appropriate and reasonable steps to keep your health information secure

Published by:

U.S. Department of Health & Human Services Office for Civil Rights

Page 2



Your Health Information Privacy Rights

Privacy is important to all of us

You have privacy rights under a federal law that protects your health information. These rights are important for you to know. You can exercise these rights, ask questions about them, and file a complaint if you think your rights are being denied or your health information isn't being protected.

Who must follow this law?

- Most doctors, nurses, pharmacies, hospitals, clinics, nursing homes, and many other health care providers
- Health insurance companies, HMOs, most employer group health plans
- Certain government programs that pay for health care, such as Medicare and Medicaid

Providers and health insurers who are required to follow this law must comply with your right to . . .

Ask to see and get a copy of your health records

You can ask to see and get a copy of your medical record and other health information. You may not be able to get all of your information in a few special cases. For example, if your doctor decides something in your file might endanger you or someone else, the doctor may not have to give this information to you.

- In most cases, your copies must be given to you within 30 days, but this can be extended for another 30 days if you are given a reason.
- You may have to pay for the cost of copying and mailing if you request copies and mailing.

Have corrections added to your health information

You can ask to change any wrong information in your file or add information to your file if it is incomplete. For example, if you and your hospital agree that your file has the wrong result for a test, the hospital must change it. Even if the hospital believes the test result is correct, you still have the right to have your disagreement noted in your file.

- In most cases the file should be changed within 60 days, but the hospital can take an extra 30 days if you are given a reason.

Receive a notice that tells you how your health information is used and shared

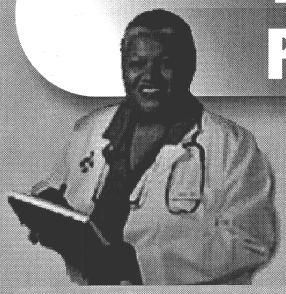
You can learn how your health information is used and shared by your provider or health insurer. They must give you a notice that tells you how they may use and share your health information and how you can exercise your rights. In most cases, you should get this notice on your first visit to a provider or in the mail from your health insurer, and you can ask for a copy at any time.

Decide whether to give your permission before your information can be used or shared for certain purposes

In general, your health information cannot be given to your employer, used or shared for things like sales calls or advertising, or used or shared for many other purposes unless you give your permission by signing an authorization form. This authorization form must tell you who will get your information and what your information will be used for.

Page 1

Your Health Information Privacy Rights



Privacy is important to all of us

Other privacy rights

You may have other health information rights under your state's laws. When these laws affect how your health information can be used or shared, that should be made clear in the notice you receive.

For more information

This is a brief summary of your rights and protections under the federal health information privacy law. You can ask your provider or health insurer questions about how your health information is used or shared and about your rights. You also can learn more, including how to file a complaint with the U.S. Government, at the website at www.hhs.gov/ocr/hipaa/ or by calling 1-866-627-7748; the phone call is free.

Published by:

U.S. Department of Health & Human Services Office for Civil Rights

Providers and health insurers who are required to follow this law must comply with your right to . . .

Get a report on when and why your health information was shared

Under the law, your health information may be used and shared for particular reasons, like making sure doctors give good care, making sure nursing homes are clean and safe, reporting when the flu is in your area, or making required reports to the police, such as reporting gunshot wounds. In many cases, you can ask for and get a list of who your health information has been shared with for these reasons.

- You can get this report for free once a year.
- In most cases you should get the report within 60 days, but it can take an extra 30 days if you are given a reason.

Ask to be reached somewhere other than home

You can make reasonable requests to be contacted at different places or in a different way. For example, you can have the nurse call you at your office instead of your home, or send mail to you in an envelope instead of on a postcard. If sending information to you at home might put you in danger, your health insurer must talk, call, or write to you where you ask and in the way you ask, if the request is reasonable.

Ask that your information not be shared

You can ask your provider or health insurer not to share your health information with certain people, groups, or companies. For example, if you go to a clinic, you could ask the doctor not to share your medical record with other doctors or nurses in the clinic. However, they do not have to agree to do what you ask.

File complaints

If you believe your information was used or shared in a way that is not allowed under the privacy law, or if you were not able to exercise your rights, you can file a complaint with your provider or health insurer. The privacy notice you receive from them will tell you who to talk to and how to file a complaint. You can also file a complaint with the U.S. Government.

Page 2

GAO Contact and Staff Acknowledgments

GAO Contact

Rosamond Katz, (202) 512-7148

Acknowledgments

In addition to the contact named above, Kelly L. DeMots, Mary F. Giffin, Eric A. Peterson, and Lisa M. Vasquez made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

United States
Government Accountability Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Service Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00