



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.

HEALTH INFORMATION

First-Year Experiences under the Federal Privacy Rule

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.