United States General Accounting Office

GAO

Testimony

Before the Committee on Health, Education, Labor, and Pensions, U.S. Senate

For Release on Delivery
Expected at 9:30 a.m.
Thursday, February 8, 2001

HEALTH PRIVACY

Regulation Enhances Protection of Patient Records but Raises Practical Concerns

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

Health Privacy: Regulation Enhances Protection of Patient Records but Raises Practical Concerns

Mr. Chairman and Members of the Committee:

We are pleased to be here today as you discuss the new federal regulation covering the privacy of personal health information. Advances in information technology, along with an increasing number of parties with access to identifiable health information, have created new challenges to maintaining the privacy of an individual's medical records. Patients and providers alike have expressed concern that broad access to medical records by insurers, employers and others may result in inappropriate use of the information. Congress sought to protect the privacy of individuals' medical information as part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[1] HIPAA included a timetable for developing comprehensive privacy standards that would establish rights for patients with respect to their medical records and define the conditions for using and disclosing identifiable health information. In December 2000, the Department of Health and Human Services (HHS) released the final regulation on privacy standards.[2] The regulation requires that most affected entities comply by February 26, 2003.[3]

In April 2000, we testified on HHS' proposed privacy regulation.[4] At that time, we noted that the comments made by the affected parties reflected two overriding themes. The first was a widespread acknowledgment of the importance of protecting the privacy of medical records. The second reflected the conflicts that arise in attempts to balance protecting patients' privacy and permitting the flow of health information for necessary uses. Last month, the Committee requested that we obtain the perspectives of affected parties regarding the regulation. My remarks today will focus on (1) the rights of patients and the responsibilities of the entities that use personal health information, as set forth in the federal privacy regulation and (2) the concerns of key stakeholders regarding the regulation's major provisions. In gathering this information, we contacted 17 national organizations representing patients, health care providers, accrediting bodies, state officials, employers, insurance companies, and research and

[1] P.L. 104-191, 264, 110 Stat. 1936, 2033.

[2] 65 *Fed. Reg.* 82,462 (2000). The regulation can also be accessed at http://aspe.hhs.gov/admnsimp/.

[3] The regulation was to become effective on February 26, 2001. However, it is unclear whether the Administration's moratorium delaying the effective dates of regulations that have been published in the *Federal Register* will apply to the HHS privacy regulation.

[4] *Privacy Standards: Issues in HHS' Proposed Rule on Confidentiality of Personal Health Information* (GAO/T-HEHS-00-106, Apr. 26, 2000).

pharmaceutical groups.[5] (A list of these organizations is in the appendix.) We also reviewed the regulation and spoke with HHS officials responsible for implementing it. We performed our work in January 2001 in accordance with generally accepted government auditing standards.

In brief, the regulation acts as a federal floor (to be superseded by state privacy regulations that are more stringent) in establishing standards affecting the use and disclosure of personal health information by providers, health plans, employers, researchers, and government agencies. Patients will have increased knowledge about, and potential control over, what information is shared, with whom, and for what purposes. At the same time, entities that receive personal health information will be responsible for ensuring that the information is effectively protected.

Most groups we interviewed acknowledged that HHS was responsive in addressing many of their comments on the draft regulation. However, given the newness, breadth, and complexity of the regulation, they also expressed uncertainty about all that organizations may need to do to comply. Many raised questions about the requirements for entities to obtain patient consent or authorization prior to disclosing or using personal health information. Other concerns focused on how regulated entities will apply the privacy provisions to their business associates. Most groups focused on the HIPAA provision that more stringent state privacy requirements preempt the federal regulation. Some groups favored this flexibility, whereas others asserted that the lack of a single set of privacy standards will add regulatory burden. Finally, many organizations raised questions about the feasibility and cost of implementing the regulation in the time allotted.

Background

The federal privacy regulation is the second of nine administrative simplification standards to be issued under HIPAA that HHS has released in final form.[6] In addition to information privacy, the standards are to address transaction codes and medical data code sets; consistent identifiers for patients, providers, health plans, and employers; claims attachments that support a request for payment; data security; and enforcement. Taken together, the nine standards are intended to

[5]In addition to interviewing selected groups, we also received information volunteered from other organizations.

[6]A regulation governing electronic transactions was issued on August 17, 2000.

streamline the flow of information integral to the operation of the health care system while protecting confidential health information from inappropriate access, disclosure, and use.

HIPAA required the Secretary of HHS to submit recommendations to the Congress on privacy standards, addressing (1) the rights of the individual who is the subject of the information; (2) procedures for exercising such rights; and (3) authorized and required uses and disclosures of such information. HIPAA further directed that if legislation governing these privacy standards was not enacted within 3 years of the enactment of HIPAA—by August 21, 1999—the Secretary should issue regulations on the matter. HHS submitted recommendations to Congress on September 11, 1997, and when legislation was not enacted by the deadline, issued a draft regulation on November 3, 1999. After receiving over 52,000 comments on the proposed regulation, HHS issued a final regulation on December 28, 2000.

Two key provisions in HIPAA defined the framework within which HHS developed the privacy regulation.

- HIPAA specifically applies the administrative simplification standards to health plans, health care clearinghouses (entities that facilitate the flow of information between providers and payers), and health care providers that maintain and transmit health information electronically. HHS lacks the authority under HIPAA to directly regulate the actions of other entities that have access to personal health information, such as pharmacy benefit management companies acting on behalf of managed care networks.[7]

- HIPAA does not allow HHS to preempt state privacy laws that are more protective of health information privacy. Also, state laws concerning public health surveillance (such as monitoring the spread of infectious diseases) may not be preempted.

[7]The regulation does not govern workers compensation carriers, life insurers, Web sites that do not provide health treatment or insurance services, and other entities that collect and maintain health information. An unknown number of providers are not covered entities because they do not electronically transmit any of the standard financial or administrative transactions specified in HIPAA. Although likely to be few overall, members of this group, including some physicians providing occupational health care for employers, could have control over sensitive patient information.

HIPAA does not impose limits on the type of health care information to which federal privacy protection would apply. At the time the proposed regulation was issued, HHS sought to protect only health data that had been stored or transmitted electronically, but it asserted its legal authority to cover all personal health care data if it chose to do so.[8] HHS adopted this position in the final regulation and extended privacy protection to personal health information in whatever forms it is stored or exchanged—electronic, written, or oral.

Privacy Regulation Establishes New Rights and Responsibilities

The new regulation establishes a minimum level of privacy protection for individually identifiable health information that is applicable nationwide. When it takes full effect, patients will enjoy new privacy rights, and providers, plans, researchers, and others will have new responsibilities.[9] Most groups have until February 26, 2003, to come into compliance with the new regulation, while small health plans[10] were given an additional year.

Patients' Rights

The regulation protecting personal health information provides patients with a common set of rights regarding access to and use of their medical records. For the first time, these rights will apply to all Americans, regardless of the state in which they live or work. Specifically, the regulation provides patients the following:

- Access to their medical records. Patients will be able to view and copy their information, request that their records be amended, and obtain a history of authorized disclosures.
- Restrictions on disclosure. Patients may request that restrictions be placed on the disclosure of their health information. (Providers may choose not to accept such requests.) Psychotherapy notes may not be used by, or disclosed to, others without explicit authorization.

[8]In our previous testimony we specifically examined HHS' legal authority to include personal health information that had never been stored or transmitted electronically. We determined that the Department was correct in its conclusion that HIPAA did not restrict the potential scope of the regulation on this basis.

[9]The Privacy Act of 1974 (5 U.S.C. 552a) established privacy protections for the use of personal health information by federal agencies.

[10]Small health plans are defined in the regulation as those with annual receipts of $5 million or less.

- Education. Patients will receive a written notice of their providers' and payers' privacy procedures, including an explanation of patients' rights and anticipated uses and disclosures of their health information.

- Remedies. Patients will be able to file a complaint with the HHS Office for Civil Rights (OCR) that a user of their personal health information has not complied with the privacy requirements.[11] Violators will be subject to civil and criminal penalties established under HIPAA.

Responsibilities of Providers, Health Plans, and Clearinghouses

Providers, health plans, and clearinghouses—referred to as covered entities—must meet new requirements and follow various procedures, as follows:

- Develop policies and procedures for protecting patient privacy. Among other requirements, a covered entity must designate a privacy official, train its employees on the entity's privacy policies, and develop procedures to receive and address complaints.

- Obtain patients' written consent or authorization. Providers directly treating patients must obtain written consent to use or disclose protected health information to carry out routine health care functions.[12] Routine uses include nonemergency treatment, payment, and an entity's own health care operations.[13] In addition, providers, health plans, and clearinghouses must obtain separate written authorization from the patient to use or disclose information for nonroutine purposes, such as releasing information to lending institutions or life insurers.[14]

[11]The regulation does not authorize patients to sue to enforce privacy standards. However, a patient may bring a claim in a state where such actions are permitted under statute or common law.

[12]A consent is written in general terms and references the notice that patients receive regarding the use of protected health information. Providers may make patient consent a condition of receiving treatment.

[13]Health care operations are a provider's or health plan's management and other activities necessary for support of treatment or payment. For example, a hospital may use personal health information to teach or train staff, conduct research on treatments, or assure quality.

[14]The regulation specifies certain situations in which providers and plans require neither a written consent nor authorization before health information is used or disclosed. Examples include health system oversight, public health activities, certain research studies, law enforcement, and facilities' patient directories (patient must be given opportunity to opt out).

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

- Ensure that "downstream users" protect the privacy of health information. Covered entities must enter into a contract with any business associates with which they share personal health information for purposes other than consultation, referral, or treatment.[15] Contracts between covered entities and their business associates must establish conditions and safeguards for uses and disclosures of identifiable health information. Covered entities must take action if they know of practices by their business associates that violate the agreement.

- Adhere to specific procedures in using information for fundraising or marketing. Covered entities may use protected patient information to develop mailing lists for fundraising appeals, but they must allow patients to choose not to receive future appeals. Similarly, while patient authorization is required to transmit personal health information to a third party for marketing purposes, a covered entity (or its business associate) can itself use such data for marketing on behalf of a third party without authorization. In such cases, the entity must identify itself as the source of the marketing appeal, state whether it is being paid to do so, and give recipients the opportunity to opt out of receiving additional marketing communications.

- Protect unauthorized release of medical records to employers. Group health plans must make arrangements to ensure that personal health information disclosed to the sponsors, including employers, will not be used for employment-related purposes, such as personnel decisions,

[15]A business associate is any person or organization that performs a function involving the use or disclosure of identifiable health information on behalf of a covered entity or provides legal, actuarial, accounting, or other services. Physicians on hospital medical staffs are not considered business associates of the hospital.

without explicit authorization from the individual.[16] Furthermore, where staff administering the group health plan work in the same office as staff making hiring and promotion decisions, access to personal health information must be limited to those employees who perform health plan administrative functions.

Responsibilities of Researchers

The regulation sets out special requirements for use of personal health information that apply to both federal and privately funded research:

- Researchers may use and disclose health information without authorization if it does not identify an individual. Information is presumed to be de-identified by removing or concealing all individually identifiable data, including name, addresses, phone numbers, Social Security numbers, health plan beneficiary numbers, dates indicative of age, and other unique identifiers specified in the regulation.

- Researchers who seek personal health information from covered entities will have two options. They can either obtain patient authorization or obtain a waiver from such authorization by having their research protocol reviewed and approved by an independent body—an institutional review board (IRB) or privacy board. In its review, the independent body must determine that the use of personal health information will not adversely affect the rights or welfare of the individuals involved, and that the benefit of the research is expected to outweigh the risks to the individuals' privacy.

Responsibilities and Rights of Federal Agencies and State Governments

HHS and others within the federal government will have a number of specific responsibilities to perform under the regulations. Although it no longer falls to the states to regulate the privacy of health information, states will still be able to enact more stringent laws.

- Federal and state public officials may obtain, without patient authorization, personal health information for public health surveillance; abuse, neglect, or domestic violence investigations; health care fraud investigations; and other oversight and law enforcement activities.

[16]Group health plans include employee welfare benefit plans (both insured and self-insured) subject to the Employee Retirement Income Security Act (ERISA). Employee health benefit plans are excluded if they have fewer than 50 participants.

- HHS' OCR has broad authority to administer the regulation and provide guidance on its implementation. It will decide when to investigate complaints that a covered entity is not complying and perform other enforcement functions directly related to the regulations. HIPAA gives HHS authority to impose civil monetary penalties ($100 per violation up to $25,000 per year) against covered entities for disclosures made in error. It may also make referrals for criminal penalties (for amounts of up to $250,000 and imprisonment for up to 10 years) against covered entities that knowingly and improperly disclose identifiable health information.

Concerns by Stakeholders Reflect Complexity of the Regulation

Among the stakeholder groups we interviewed, there was consensus that HHS had effectively taken into account many of the views expressed during the comment period. Most organizations also agreed that the final regulation improved many provisions published in the proposed regulation. At the same time, many groups voiced concerns about the merit, clarity, and practicality of certain requirements.

Overall, considerable uncertainty remains regarding the actions needed to comply with the new privacy requirements. Although the regulation, by definition, is prescriptive, it includes substantial flexibility. For example, in announcing the release of the regulation, HHS noted that "the regulation establishes the privacy safeguard standards that covered entities must meet, but it leaves detailed policies and procedures for meeting these standards to the discretion of each covered entity." Among the stakeholder groups we interviewed, the topics of concern centered on conditions for consent, authorization, and disclosures; rules pertaining to the business associates of covered entities; limited preemption of state laws; the costs of implementation; and HHS' capacity to provide technical assistance.

Consent and Disclosure Provisions Attracted a Range of Concerns

Several of the organizations we contacted considered the regulation's consent, authorization, or disclosure provisions a step forward in the protection of personal health information. However, several groups questioned the merits of some of the provisions. For example, representatives of patient advocacy groups—the National Partnership for Women and Families, the Health Privacy Project, and the American Civil Liberties Union—were concerned that the regulation permits physicians, hospitals, and other covered entities to market commercial products and services to patients without their authorization. One representative noted that commercial uses of patient information without authorization was an issue that provided the impetus for federal action to protect health privacy

in the first place. Another representative commented that public confidence in the protection of their medical information could be eroded as a result of the marketing provisions. One representative also concluded that allowing patients the opportunity to opt out in advance of all marketing contacts would better reflect the public's chief concern in this area. HHS officials told us that this option exists under the provision granting patients the right to request restrictions on certain disclosures but that providers are not required to accept such patient requests.

Several organizations questioned whether the scope of the consent provision was sufficient. For example, American Medical Association (AMA) representatives supported the requirement that providers obtain patient consent to disclose personal health information for all routine uses, but questioned why the requirement did not apply to health plans. Plans use identifiable patient information for quality assurance, quality improvement projects, utilization management, and a variety of other purposes. The association underscored its position that consent should be obtained before personal health information is used for any purpose and that the exclusion of health plans was a significant gap in the protection of this information. AMA suggested that health plans could obtain consent as part of their enrollment processes.

The American Association of Health Plans (AAHP) also expressed concerns about the scope of consent, but from a different perspective. AAHP officials believe that the regulation may limit the ability of the plans to obtain the patient data necessary to conduct health care operations if providers' patient consent agreements are drawn too narrowly to allow such data sharing. They suggested two ways to address this potential problem. First, if the health plans and network providers considered themselves an "organized health care arrangement,"[17] access to the information plans needed could be covered in the consent providers obtained from their patients. Second, plans could include language in their contracts with physicians that would ensure access to patients' medical record information.

Several organizations also had questions about how the consent requirement might be applied. For example, the American Pharmaceutical Association (APhA) raised concerns about how

[17]An organized health care arrangement involves clinical or operational integration among legally separate covered entities, which often need to share protected health information for the joint management and operations of the arrangement.

pharmacies could obtain written consent prior to treatment—that is, filling a prescription for the first time. The American Health Information Management Association (AHIMA) similarly noted the timing issue for hospitals with respect to getting background medical information from a patient prior to admission. HHS officials told us that they believe the regulation contains sufficient flexibility for providers to develop procedures necessary to address these and similar situations.

Research organizations focused on the feasibility of requirements for researchers to obtain identifiable health information. The regulation requires them to obtain patient authorization unless an independent panel reviewing the research waives the authorization requirement.[18] Although this approach is modeled after long-standing procedures that have applied to federally funded or regulated research,[19] the regulation adds several privacy-specific criteria that an institutional review board or privacy board must consider. The Association of American Medical Colleges and the Academy for Health Services Research and Health Policy expressed specific concerns over the subjectivity involved in applying some of the additional criteria. As an example, they highlighted the requirement that an independent panel determine whether the privacy risks to individuals whose protected health information is to be used or disclosed are reasonable in relation to the value of the research involved.

Relationships Uncertain Regarding Covered Entities and Their Business Associates

Several groups were concerned about the requirement for covered entities to establish a contractual arrangement with their business associates—accountants, attorneys, auditors, data processing firms, among others—that includes assurances for safeguarding the confidentiality of protected information. This arrangement was HHS' approach to ensure that the regulation's protections would be extended to information shared with others in the health care system. Some provider groups we spoke with were confused about the circumstances under which their member organizations would be considered covered entities or business associates.

Some groups, including the Health Insurance Association of America (HIAA) and the Blue Cross and Blue Shield Association (BCBSA),

[18]Authorization is not required for "de-identified" information. However, several organizations were concerned that the regulation's provisions for de-identification specify the removal of information that could be important for research purposes, such as a patient's county, city, or zip code.

[19]The Federal Policy for the Protection of Human Subjects, referred to as the Common Rule, describes conditions under which research may be conducted without obtaining an individual's authorization to use identifiable health information.

questioned the need for two covered entities sharing information to enter into a business associate contract. The regulation addresses one aspect of this concern. It exempts a provider from having to enter into a business associate contract when the only patient information to be shared is for treatment purposes. This exemption reflects the reasoning that neither entity fits the definition of business associate when they are performing services on behalf of the patient and not for one another. An example of such an exemption might include physicians writing prescriptions to be filled by pharmacists.

Some groups also commented on the compliance challenges related to the business associate arrangement. For example, the representatives of the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) noted that it would need to enter into contracts for each of the 18,000 facilities (including hospitals, nursing homes, home health agencies, and behavioral health providers) that it surveys for accreditation. However, JCAHO officials hope to standardize agreements to some extent and are working on model language for several different provider types. They explained that, because assessing quality of care varies by setting, JCAHO would need more than one model contract.

Views Divided on Partial Preemption of State Laws

Most of the groups we interviewed cited as a key issue the HIPAA requirement that the privacy standards preempt some but not all state laws. Although every state has passed legislation to protect medical privacy, most of these laws regulate particular entities on specific medical conditions, such as prohibiting the disclosure of AIDS test results. However, a few states require more comprehensive protection of patient records. The patient advocacy groups we spoke with believe that partial preemption is critically important to prevent the federal rule from weakening existing privacy protections. According to the Health Privacy Project, the federal regulation will substantially enhance the confidentiality of personal health information in most states, while enabling states to enact more far-reaching privacy protection in the future.

Despite the limited scope of most state legislation at present, other groups representing insurers and employers consider partial preemption to be operationally cumbersome and argue that the federal government should set a single, uniform standard. Organizations that operate in more than one state, such as large employers and health plans, contend that determining what mix of federal and state requirements applies to their operations in different geographic locations will be costly and complex.

Although they currently have to comply with the existing mix of state medical privacy laws, they view the new federal provisions as an additional layer of regulation.[20] A representative of AHIMA remarked that, in addition to state laws, organizations will have to continue to take account of related confidentiality provisions in other federal laws (for example, those pertaining to substance abuse programs) as they develop policies and procedures for notices and other administrative requirements.

The final regulation withdrew a provision in the proposed regulation that would have required HHS to respond to requests for advisory opinions regarding state preemption issues. HHS officials concluded that the volume of requests for such opinions was likely to be so great as to overwhelm the Department's capacity to provide technical assistance in other areas. However, they did not consider it unduly burdensome or unreasonable for entities covered by the regulation to perform this analysis regarding their particular situation, reasoning that any new federal regulation requires those affected by it to examine the interaction of the new regulation with existing state laws and federal requirements.

Stakeholders Believe Compliance Challenges May Be Costly

Several groups in our review expressed concern about the potential costs of compliance with the regulation and took issue with HHS' impact analysis. In that analysis, the Department estimated the covered entities' cost to comply with the regulation to be $17.6 billion over the first 10 years of implementation. Previously, HHS estimated that implementation of the other administrative simplification standards would save $29.9 billion over 10 years, more than offsetting the expenditures associated with the privacy regulation. HHS therefore contends that the regulation complies with the HIPAA requirement that the administrative simplification standards reduce health care system costs.

HHS expects compliance with two provisions—restricting disclosures to the minimum information necessary and establishing a privacy official—to be the most expensive components of the privacy regulation, in both the short and the long term. Table 1 shows HHS' estimates of the costs to covered entities of complying with the privacy regulation.

[20]In the case of employee health plans, which are covered by ERISA, the federal preemption of state laws that "relate to" those plans will continue to apply. Therefore, a state law that established more stringent privacy protections than the federal privacy regulation may or may not supplant the regulation for ERISA plans in the state, depending on the facts and circumstances involved.

Table 1: HHS' Cost Estimates for Implementing the Privacy Regulation

(Millions of Dollars)

Requirements	First-year costs (2003)	10-year costs (2003-12)
Disclose only minimum necessary information	$926.2	$5,756.7
Designate a privacy official	723.2	5,905.8
Develop policies and procedures	597.7	597.7
Establish business associate contracts	299.7	800.3
Train employees in privacy policies	287.1	737.2
Track authorized disclosures	261.5	1,125.1
Obtain consent to use patient information	166.1	227.5
De-identify protected health information	124.2	1,177.4
Modify health information for employer use (applies to group health plans)	52.4	52.4
Prepare and distribute notice of privacy practices	50.8	391.0
Obtain IRB or privacy board approval for research	40.2	584.8
Implement a process for individuals to file complaints	6.6	103.2
Amend patient medical records on request	5.0	78.8
Process patient requests to inspect and copy their medical records	1.3	16.8
Total	**3,542.0**	**17,554.7**

Source: *Federal Register,* Dec. 28, 2000, page 82761.

We did not independently assess the potential cost of implementing the privacy regulation, nor had the groups we interviewed. However, on the basis of issues raised about the regulation, several groups anticipate that the costs associated with compliance will exceed HHS' estimates. For example, BCBSA representatives contended that its training costs are likely to be substantial, noting that its member plans encompass employees in a wide range of positions who will require specialized training courses. AHA cited concerns about potentially significant new costs associated with developing new contracts under the business associate provision. Other provider groups anticipated spending additional time with patients to explain the new requirements and obtain consent, noting that these activities will compete with time for direct patient care. Several groups, including AHA, AAMC, and AHIMA, expressed concerns about being able to implement the regulation within the 2-year time frame.

Despite their concerns, several groups discussed possible actions that could help mitigate the anticipated administrative burden. For example, AHA plans to develop model forms for patient consent forms, notices explaining privacy practices, business associate contracts, and compliance plans. Representatives of APhA similarly intend to give their members

model forms, policies, and procedures for implementing the regulation. AMA expects to provide guidance to physicians and help with forms and notices on a national level, and noted that the state medical associations are likely to be involved in the ongoing analysis of each state's laws that will be required.

HHS' Capacity to Assist With Implementation Questioned

Representatives of some organizations we contacted commented that they were unsure how the Department's OCR will assist entities with the regulation's implementation. They anticipate that the office, with its relatively small staff, will experience difficulty handling the large volume of questions related to such a complex regulation. OCR officials informed us that the office will require additional resources to carry out its responsibilities and that it is developing a strategic plan that will specify both its short- and its long-term efforts related to the regulation.

To carry out its implementation responsibilities, HHS requested and received an additional $3.3 million in supplemental funding above its fiscal year 2001 budget of approximately $25 million. According to OCR, this amount is being used to increase its staff of 237 to support two key functions: educating the public and those entities covered by the rule about the requirements and responding to related questions. OCR officials told us that its efforts to date include presentations to about 20 organizations whose members are affected by the regulation, a hotline for questions, and plans for public forums.

OCR officials said the office had received about 400 questions since the regulation was issued. Most of these inquiries were general questions relating to how copies of the regulation can be obtained, when it goes into effect, and whether it covers a particular entity. Other questions addressed topics such as the language and format to use for consent forms, how to identify organized health care arrangements, whether the regulation applies to deceased patients, and how a patient's identity should be protected in a physician's waiting room. According to OCR officials, technical questions that cannot be answered by OCR staff are referred to appropriate experts within HHS.

Conclusion

The final privacy regulation represents an important advancement in the protection of individuals' health information. It offers all Americans the opportunity to know and, to some extent, control how physicians, hospitals, and health plans use their personal information. At the same time, these entities will face a complex set of privacy requirements that are not well understood at this time. Some of the uncertainty expressed

by stakeholder groups reflects the recent issuance of the regulation. With time, everyone will have greater opportunity to examine its provisions in detail and assess their implications for the ongoing operations of all those affected. In addition, on a more fundamental level, the uncertainty stems from HHS' approach of allowing entities flexibility in complying with its requirements. Although organizations generally applaud this approach, they acknowledge that greater specificity would likely allay some of their compliance concerns.

Mr. Chairman and Members of the Committee, this concludes my prepared statement. I will be happy to answer any questions you may have.

GAO Contact and Acknowledgments

For future contacts regarding this testimony, please call Leslie G. Aronovitz, Director, Health Care—Program Administration and Integrity Issues, at (312) 220-7600. Other individuals who made contributions to this statement include Hannah Fein, Jennifer Grover, Joel Hamilton, Rosamond Katz, Eric Peterson, Daniel Schwimer, and Craig Winslow.

Organizations Interviewed

We included the following organizations in our review:

American Association of Health Plans
American Benefits Council
Academy for Health Services Research and Health Policy
American Civil Liberties Union
American Health Information Management Association
American Hospital Association
American Medical Association
American Pharmaceutical Association
Association of American Medical Colleges
Blue Cross and Blue Shield Association
Health Insurance Association of America
Health Privacy Project
Joint Commission on Accreditation of Healthcare Organizations
Merck-Medco Managed Care, L.L.C.
National Association of Insurance Commissioners
National Partnership for Women and Families
Pharmaceutical Research and Manufacturers of America

(290019)

Ordering Information

Orders by Internet

For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

Info@www.gao.gov

or visit GAO's World Wide Web home page at:

http://www.gao.gov

To Report Fraud, Waste, and Abuse in Federal Programs

Contact one:

Web site: http://www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

1-800-424-5454