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 10:00 a.m.
Wednesday, April 26, 2000

PRIVACY STANDARDS

Issues in HHS' Proposed Rule on Confidentiality of Personal Health Information

Statement of Janet Heinrich, Associate Director
Health Financing and Public Health Issues
Health, Education, and Human Services Division

Privacy Standards: Issues in HHS' Proposed Rule on Confidentiality of Personal Health Information

Mr. Chairman and Members of the Committee:

We are pleased to be here today to discuss the most recent efforts to develop a federal health privacy policy. Few areas of our lives are perceived to be more private than our health and medical care. Historically, individuals' access to information contained in their own medical records and control of others' access to that information have largely been in the command of patients, their physicians, and providers such as hospitals. However, the proliferation of electronic records and managed care arrangements has raised questions about the extent to which individuals' health care information is protected from inappropriate disclosure. The disclosure of personally identifiable medical information without authorization may not only result in information being revealed that an individual wishes to remain confidential but may subject an individual to discrimination in employment, insurance, or other matters.

While federal statutes affect the disclosure of records under federally funded programs—such as the Medicare program or veterans' programs—no comprehensive federal laws have been enacted covering private sector activities in this area. Recognizing the need to ensure confidentiality of patient data, the Congress included in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) a provision that the Secretary of Health and Human Services develop legislative recommendations aimed at filling this gap.[1] The Congress further stipulated that if legislation governing privacy standards was not enacted by August 21, 1999, the Secretary should issue regulations on the matter. The Department of Health and Human Services (HHS) submitted the required recommendations to the Congress, but legislation was not enacted. HHS issued proposed regulations on November 3, 1999.[2]

You asked us to examine the proposed regulation in terms of HHS' legal authority to act in this area as well as assess the reaction from interested parties. Specifically, we (1) examined the authoritative basis in the HIPAA statute for some of the approaches taken by HHS in the proposed rule, (2) assessed the overall pattern of public responses to the rule among a selected group of 40 organizations representing different constituencies

[1]HIPAA required the Secretary of Health and Human Services to submit recommendations to the Congress on privacy standards for individually identifiable health information addressing at least the following: (1) 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.

[2]64 *Fed. Reg.* 59,918. (Hereafter, "proposed rule" or "proposed regulations.") The proposed rule can be accessed at http://aspe.hhs.gov/adminsimp

affected by the rule, (3) examined in detail the content of the views expressed by those organizations with respect to six sections of the rule that prompted an especially large volume of comments, and (4) identified concerns that would require legislative action to address.

In addressing these objectives, we examined the proposed rule and the comments submitted in response to it by a selected group of 40 organizations.[3] In constructing this list, we tried to incorporate those organizations that had been active on this issue in the past, as well as provide broad representation of different constituencies potentially affected by the rule. Thus, the list includes organizations representing patients, health care providers, standards and accrediting bodies, government entities, health care clearinghouses, employers, health plans, and research and pharmaceutical groups. (A list of these organizations is in the app.)

With regard to HHS' statutory authority, we reviewed three issues that you identified as potentially problematic: (1) controlling the use of information by others not specifically covered by HHS' proposed rule ("downstream users") by requiring covered entities to enter into contracts with business partners; (2) the extension of protection to the paper versions of electronic data; and (3) the "scalability" standard, which permits different covered entities to decide, on the basis of a judgment of their administrative capacity, how much they need to do to comply with the regulations. In our review of the 40 stakeholders' comments, we abstracted the positions that each took on the more than 50 sections of the proposed rule. From this we determined which sections of the rule generated comments from the different categories of organizations among our 40 selected stakeholders. We then conducted a more detailed analysis of the six sections of the rule that we found had attracted the greatest overall interest. We also took particular note of any recommendations that would require legislation before they could be implemented.

In brief, the regulatory strategies HHS adopted in the proposed rule seem consistent with HIPAA's purpose of protecting the privacy of health information and are legally permissible. By requiring that entities directly regulated by the rule—health plans, health care providers, and health care clearinghouses (firms that put information into standard formats)—control the information practices of entities with which they do business, HHS has attempted to fill an otherwise significant gap in privacy protection. For the same reason, HHS has covered the "paper progeny" of

[3]Also referred to as "stakeholders" or "commenters."

electronically maintained or transmitted health information—the privacy protections extended to individuals by HIPAA would be easy to circumvent if protected health information in an electronic record lost its protection merely by being printed. HHS' decision to build flexibility into the proposed rule by allowing implementation of the standards to vary on the basis of an organization's size is also within its authority.

The stakeholders' comments to HHS reflected sharply divergent views on several critical issues. Most notably, patient advocates, state government representatives, and providers strongly supported the provision of the rule that preempts weaker state laws while leaving intact stronger ones. Meanwhile, health plans and employers emphasized the practical difficulties of implementing the complex interaction of federal and different state standards. Similarly, patient advocates and law enforcement officials approved of extending the rule's coverage from the three types of entities subject to HIPAA regulation to business partners with whom these entities share protected health care data. However, the covered entities themselves were wary of assuming the responsibility for enforcing compliance by these other groups. In some cases, the changes desired by industry groups and patient advocates would require congressional action. For example, HHS could not establish a uniform federal privacy standard preempting all applicable state laws unless HIPAA was amended. Similarly, only the Congress could expand the rule's coverage to all types of entities that create, use, and share protected health information. For other proposed changes, such as coverage of records that had never been stored or transmitted electronically, it was less clear whether HHS could act without new legislation.

Background

Highlights of the Proposed Rule

The proposed regulation addresses the protection of health information from its creation and establishes uniform requirements for those handling the information. Personal health information may be used and disclosed under conditions specified in the rule or when the individual authorizes it, and it must be disclosed when the individual wants to review his or her own information (and when the Secretary wants to look at the information to enforce the rule). Key elements of the proposed regulation are shown in table 1.

Table 1: Key Provisions of the Proposed Privacy Regulation

Entities the regulation covers	Covered entities are all health plans, health care providers, and health care clearinghouses.
Information the regulation covers	Covered information is any that has been maintained electronically or transmitted electronically. Such information is protected in all its manifestations, including its printed form, when it is held by a covered entity.
Permitted uses without individual authorization	•Protected information may be used and disclosed for treatment, payment, and health care operations. •Plans and providers must have contracts with their business partners (lawyers, accountants, third-party administrators, accrediting organizations, and others who perform services on behalf of a plan or provider) that limit how they may use the information. Covered entities may be held responsible for the transgressions of their business partners. •Information may be used without individual authorization for public policy purposes such as research, public health monitoring, health care oversight, and law enforcement.
Information practices	•When covered entities disclose information, they may disclose only the minimum amount necessary to fulfill the purpose. Such determinations are to be made on a case-by-case basis, when technologically feasible. •Covered entities can meet privacy standards by removing specified identifying data elements. •Covered entities must provide up-to-date notice to patients and enrollees describing their rights and how the entity intends to use or disclose the information. •A covered entity may not condition treatment or payment on obtaining an authorization for a disclosure for a nonrelated purpose (such as marketing). •Covered entities must provide individuals on request with an accounting of disclosures of their identifiable health information.
Individual rights	•Individuals have a right to inspect and copy their medical records. Individuals also have a right to amend and correct erroneous health information. •Individuals have a right to request restrictions on further uses or disclosures of their identifiable health information in certain instances. •Individuals may file complaints with a covered entity and with the Secretary of Health and Human Services about possible privacy rule violations.
Administrative requirements	•Covered entities must have a designated privacy official to oversee privacy practices. •Covered entities must develop and apply sanctions when appropriate to employees and business partners who misuse information. •Covered entities must also develop and document their policies and procedures for implementation of rule requirements.
Preemption	The proposed rule preempts state laws that are contrary to the rule**,** with certain exceptions. Exceptions include state laws that are more stringent, public health surveillance laws, and parental access laws.
Enforcement	HHS may make a formal finding of noncompliance and use it as a basis to initiate an action under HIPAA or to refer the matter to the Department of Justice for prosecution under HIPAA. HIPAA sets forth civil and criminal penalties for violations.

HHS Process for Obtaining Input on the Proposed Regulation

Although proposed regulations generally have a 60-day comment period, HHS extended the time period for submitting comments on the privacy regulations for an additional 45 days at the request of several health care groups. During the 3-½-month comment period, HHS received just under 52,000 comments. Some groups organized campaigns to promote public comment on the regulation: 30,000 letters from one group were essentially identical, while 10,500 submitted by another organization were more varied but endorsed similar themes. In accordance with the Administrative Procedure Act, all comments are being reviewed and summarized for inclusion in the preamble to the final rule. According to an HHS senior policy adviser, the target date for publication of the final rule is not known. The rule would be effective 26 months after the final rule is published.

HHS' Exercise of Its Rulemaking Authority Is Consistent With HIPAA

Under HIPAA, HHS' authority to issue regulations is limited to setting standards for three specific types of entities: health plans, health care clearinghouses, and health care providers that transmit information electronically in connection with specific financial and administrative transactions. In the preamble to the proposed regulations, HHS acknowledges that, because of this limitation, it lacks authority to implement comprehensive privacy protections and therefore it did not attempt to do so. Because of concerns that the regulation would leave gaps in protection, HHS has attempted to find ways, consistent with the statute, to protect privacy even where it cannot regulate directly. Some have suggested that HHS has gone beyond what the law authorizes in parts of the proposed rule, while elsewhere it has left too much leeway to the regulated entities to decide how to comply with the proposed standards. Specifically, questions have been raised about (1) requiring covered entities to get assurances that their business partners—"downstream" users of the data—will safeguard the information; (2) extending privacy protection to the contents of electronic records in other forms (such as printouts); and (3) partly on the basis of their size and the nature of their business, allowing some regulated entities to decide the detailed policies and procedures for complying with the proposed regulations (HHS refers to this as "scalability").

We found that in these areas HHS did not exceed its statutory authority. HHS has broad authority to decide how to administer programs for which it is responsible and to interpret the statutes establishing those programs, such as HIPAA. In developing the proposed regulations, HHS has used this authority to regulate areas in which it reads the law as leaving room for discretion.

Requiring Safeguards by Business Partners

The proposed regulations would require covered entities (health plans, health care clearinghouses, and any health care providers that transmit health information in electronic form) to get assurances from business partners that they in turn will safeguard the information. Business partners include lawyers, auditors, consultants, data processing firms, and others to whom the covered entity discloses protected health information so that the business partner can carry out a function of the covered entity.

The assurance required is a written contract explicitly limiting the business partner's uses and disclosure of the information and imposing security, inspection, and reporting requirements on the business partner. The regulations further protect the information in the hands of downstream users by requiring the business partner to ensure that any subcontractors or agents to whom it provides protected health information will agree to the same restrictions and conditions that apply to the business partner. The covered entity is to be held responsible for any of the business partner's material breaches of the contract if the covered entity either knew of them, or reasonably should have known, and failed to take reasonable steps to remedy them.

We find these provisions to be reasonable and within HHS' authority to promulgate. They are consistent with HIPAA's purpose of protecting the privacy of individually identifiable health information; without some control over downstream use, the protection afforded by the rule would be significantly weakened. The business partner provisions fill a gap left by HIPAA by providing needed protection not explicitly provided for by the statute, without directly imposing requirements on entities not covered by the statute.

In proposing this part of the rule, HHS recognized that many of those who would likely obtain personally identifiable health information from covered entities are not themselves entities covered by the statute and that it did not have authority to directly regulate their use of the information. Although HHS would be acting beyond its HIPAA authority if it attempted directly to regulate entities not covered by the statute, that is not the case here: the proposed regulations distinguish clearly between treatment of covered entities and treatment of business partners. First, the requirements to be imposed on business partners arise only if a party voluntarily chooses to do business with a covered entity. Second, business partners are not subject to enforcement action by HHS; HHS' enforcement authority is limited to covered entities. Third, the safeguards being required of business partners are not as extensive as those the regulations would require of covered entities. For example, business partners, unlike

covered entities, are not required to develop and distribute an explanation of their privacy practices to individuals.

If someone to whom a covered entity disclosed information in the course of business could disclose it further with impunity, the protection afforded would be worth little. HHS therefore proposed this obligation for covered entities to exercise control by contract over use of information provided by them to business partners.

Extending Protection to the Paper Record of Electronic Data

Another issue that has been raised is whether HHS has authority under HIPAA to regulate nonelectronic records as well as electronic data. The proposed rule applies standards of protection to information that has been electronically transmitted or maintained by a covered entity, including such information in any other form. Thus, the regulations would apply when the electronic information is printed, discussed orally, or otherwise changed in form. The regulations also apply to the original paper version of information that is subsequently transmitted electronically.

We find nothing in HIPAA that restricts HHS' rulemaking authority related to identifiable health records to electronic data only. HHS states in the preamble to the proposed rule that it has authority under HIPAA to set privacy standards that apply to all individually identifiable health information, including information in a nonelectronic form. The privacy protections afforded individuals by HIPAA would in effect be negated if health information lost its protection merely by being printed or read aloud.

The rule was issued under authority in the law that, while referring to electronic exchanges, is not unequivocally limited to such exchanges. HHS is to issue regulations concerning "standards with respect to the privacy of individually identifiable health information transmitted in connection with [transactions described in a list, in another section of the law]." As HHS points out, this language is not, on its face, limited to electronic transmissions of individually identifiable health information, although electronic transmissions are clearly within its scope.

HHS' approach to this issue is reasonable and balanced. Although HHS believes that it has authority to issue regulations covering individually identifiable health information in any form, it limited the proposed regulations to individually identifiable health information that is at some point electronically maintained and transmitted by a covered entity. HHS explains that this approach focuses most on the primary concern of HIPAA—the effect on confidentiality of health care information of the

growing use of computerization in health care, including electronic transfers.

Scalability

Another area of the regulation about which questions have been raised is "scalability." "Scalability" refers to allowing covered entities, which vary greatly in size, to decide for themselves the detailed policies and procedures they will use in complying with various privacy standards. It has been suggested that such a practice is problematic in that it leaves to the covered entity the decision of how to comply.

HHS explained in the preamble to its proposed regulation that the standards are to be implemented by all covered entities, from a small, single-physician practice to the largest multistate health plan. HHS' approach is to propose the privacy principles and standards that covered entities must meet but to leave detailed policies and procedures for meeting the standards to the discretion of the covered entities. Furthermore, while all covered entities must meet the standards and are subject to the penalties in HIPAA, HHS said it intends the implementation of the proposed rules to be flexible and scalable in order to account for the nature of the covered entities' businesses as well as the covered entities' size and resources.[4]

An example of the application of "scalability" is that the proposed regulations require each covered entity to designate a "privacy official" to develop privacy policies but allow the entity to decide for itself details such as whether the official would have other duties not related to privacy. HHS observed that a small office might designate the office manager, who has a variety of administrative duties, as the privacy official, whereas a large entity might designate a person whose sole responsibility is privacy policy. Similarly, the regulations require covered entities to have a mechanism for receiving complaints from individuals regarding compliance with the privacy regulations, but they leave it up to the entities to decide what that mechanism is. A smaller entity might have a more informal process than a larger entity.

HHS' decision to build flexibility and scalability into the proposed rule to account for differences in entity size is within its authority. The agency's approach requires compliance with the standards by all covered entities,

[4]HHS did this, in part, to comply with the Regulatory Flexibility Act, which requires among other things that agencies take and document steps to minimize the significant economic impact of their proposed rules on small entities. In its initial regulatory flexibility analysis, HHS stated that its guiding principle concerning how to address the burden on small entities has been to make the provisions scalable.

while allowing each covered entity to devise its strategy to protect privacy information.

Support for Privacy Protection Is Widespread, While Most Concerns Focused on Certain Key Provisions

In reviewing the comments submitted by 40 selected stakeholders representing diverse affected constituencies in the medical privacy debate, we found widespread support for the goal of protecting individually identifiable health information from misuse. For this group, the issue is not whether to protect medical records privacy but what is the best approach for achieving it. Their comments indicated much implied agreement and several areas of explicit disagreement with the proposed regulation.

There were many sections of the rule that elicited little reaction—suggesting a relative lack of controversy—although other groups not included in our review could well take a different position. Areas of the rule attracting the least concern (four or fewer groups) included fairly specialized sections (such as application to military services) as well as sections of potentially broader impact (such as treatment of minors and disclosures in emergency circumstances). Fewer than 10 of the 40 stakeholders had anything to say about how the regulation addressed such issues as designation of a privacy official, disclosures for banking and payment processes, and disclosures for public health activities. A somewhat larger group (10 to 15 organizations) commented on the sections covering health oversight activities, enforcement, and compliance, and on the lengthy policies and procedures section.

Only 14 sections were commented on by at least half (20) of the stakeholders in our group, with six sections drawing the greatest attention. (See table 2.) These were provisions that would (1) preempt state laws that are in conflict with the rule and provide less stringent privacy protections; (2) allow standing authorization for disclosures for treatment, payment, or health care operations; (3) restrict the amount of information used and disclosed to the "minimum necessary"; (4) identify the entities and types of health information covered by the rule; (5) specify procedures for individual authorizations where they are still required; and (6) set provisions for business partner contracts to ensure that disclosed information remains confidential.

Table 2: Topics of Chief Concern to 40 Selected Stakeholders

Section of proposed privacy regulations	Number of organizations addressing section in their comments
Relationship to state laws	34
Disclosure for treatment, payment, and health care operations	34
"Minimum necessary" disclosure	34
Covered information and covered entities	34
Disclosure requiring individual authorization	32
Business partner agreements	31
Removal of identifying information	25
Right to request restrictions	25
Accounting for disclosures of information	24
Disclosure for research	23
Written notice of information practices	23
Inspection and copying of records	23
Amendment and correction of records	21
Disclosure for law enforcement	20

Six sections generating comments by the most stakeholders are distinguished by the breadth of interest across the 40 organizations included in our review. With one exception, they drew comments from all or nearly all of the groups in six or seven of the eight stakeholder categories.[5] By contrast, the remaining sections in table 2 engaged the interest of some stakeholder categories more than others. The section on protecting privacy by removing identifying information drew extensive comments from four of the eight categories of stakeholders. None of the other sections listed in table 2 attracted this level of interest in more than three of the eight stakeholder categories. For example, extensive comments on disclosures for research purposes were limited to research and pharmaceutical groups plus health care clearinghouses and providers. Patient advocates, government entities, and health care providers were most active in providing comments for the section on law enforcement.

[5]Stakeholders fell into the following categories: patient advocates, health care providers, standards and accrediting organizations, governmental entities, health care clearinghouses, employers, health plans, and research and pharmaceutical groups.

Comments on Most Controversial Sections Indicated Disagreement on Scope and Feasibility

In summarizing the content of the comments, we focused on the six sections of the proposed rule that attracted the most comments from all types of stakeholders. As noted above, of the more than 50 sections of the proposed regulation, only these six drew comments from at least three-quarters of the stakeholders we examined. The positions taken on these controversial sections addressed fundamental issues such as the scope of protected information and the responsibilities of different groups to safeguard that information, as well as the consequences of those decisions on the costs and burdens imposed by the rule.

Preemption of State Laws

Thirty-four of the 40 stakeholders addressed the provision that the rule would serve as a federal floor of protection rather than preempting all state laws. The proposed rule will not preempt current or future state laws if they are "more stringent than" the regulation.[6] States may apply to the Secretary of Health and Human Services for waivers from federal preemption; the regulation sets out applicable categories of exceptions. The Secretary may also issue advisory opinions—at the request of a state or on her own initiative—as to whether a provision of state law constitutes an exception because it is more stringent than the regulation.

The overriding comment, made by more than half of those remarking on this section, was that the federal rule should preempt state laws and regulations to create a single, national standard for handling health information. This position was made by all of the health plans, health care clearinghouses, and employers whose comments we reviewed. Recognizing that HIPAA does not allow HHS regulations to supersede state laws that provide greater privacy protections, several of these organizations called for congressional action to overcome this legislative restriction on HHS.

In contrast, eight other groups, including patient advocates, state government representatives, and providers, indicated support for partial federal preemption as provided in the proposed rule. They argued that it is appropriate to establish a federal floor so that rights already granted by state legislatures are not revoked and that states remain free to address future privacy concerns. Some comments focused on the value of applying the strongest privacy policy, whether it derived from federal or state law. Others particularly favored the state role in this area, with some asserting

[6]The proposed rule would not preempt several categories of state laws, including those relating to reporting of disease, injury, or child abuse; birth and death reporting; public health investigation and reporting; and laws designed to prevent fraud and abuse.

that certain additional categories of state laws should always take precedence over the proposed rule.[7]

Many of the organizations criticized the provision for partial federal preemption of state law as overly burdensome or excessively costly to implement. In particular, they asserted that substantial expense would be incurred in reviewing state laws and determining whether a state law or the proposed rule is applicable in any given situation. The Blue Cross Blue Shield Association noted that "covered entities will be unable to navigate the labyrinth of state privacy laws under the complex construct of the HIPAA regulatory model."

Several stakeholders also complained that the language in the proposed regulation was vague and confusing. One issue mentioned was how to define a stronger protection in state law. As the Healthcare Leadership Council put it, "many state laws are enacted as part of a complete initiative, where some provisions are less protective because others are more protective." This argument was amplified in calls for the regulation to further clarify the statutory terms "provision," "state law," "contrary," "relates to," and "more stringent." Some stakeholders specifically asked the Secretary to issue state-by-state preemption guidance so that covered entities could avoid making potentially erroneous preemption decisions.

The lack of preemption guidance was of particular concern to health plans and providers, given that the regulation allows only states to ask for exceptions to preemption and preemption advisory opinions. Several stakeholders suggested that HHS should be required to respond to requests for advisory opinions and exception determinations in a timely manner. Timely publication or public notice of these opinions and determinations was also cited as important. Because HHS may not be able to handle the volume of exception determination requests, both the National Association of Insurance Commissioners and the National Conference of State Legislatures requested that state law be presumed to qualify for exception from preemption until HHS makes a determination to the contrary.

[7]Specifically cited were state public safety laws; psychotherapist/patient privilege and "duty to warn" case law and statutes; state laws providing exceptions to inspection/copying requirements; access privilege laws protecting attorney-client communications and quality assurance, medical appeals, peer review, credentialing, and corporate compliance activities; and state regulatory functions not specifically listed (market conduct examinations, enforcement investigations, and consumer complaint handling).

Covered Information and Covered Entities

The applicability section of the regulation specifies which entities are covered and which information is protected. Because HIPAA provides that the regulation applies only to health plans, health care clearinghouses, and any health care providers that transmit health information in electronic form, HHS does not have the authority to apply these standards directly to any other entities.[8] The rule applies only to "protected health information," defined as identifiable information that is electronically maintained or transmitted by a covered entity, and such information in any other form.

Nearly half of all the groups commenting on this section made the same point: the rule also should protect health information in paper records that had not been maintained or transmitted electronically. At least one organization in almost every category mentioned a need to extend the scope of the rule to all individually identifiable health information, including purely paper records. These organizations generally believe that this distinction is not only less protective of privacy but also unworkable. In contrast, several commenters want a definition of protected health information that excludes pure paper records. Some of these groups suggested that HHS' authority only extends to the electronic transmission of information, not to the information's form before or after the transmission. A few stakeholders asserted that HHS' authority over health information does not extend beyond the nine standard HIPAA transactions.[9]

Although many groups contended that all information regarding a patient that is maintained by a covered entity should be subject to the rule, almost as many commenters asserted that the health information definitions under the rule should not be construed broadly. For the most part, these latter stakeholders, primarily research groups, clearinghouses, and health plans, were concerned that broad definitions have the potential to impede the delivery and quality of health care. BlueCross BlueShield, for example, suggested that protected information exclude all information that does not relate to an actual medical record, asserting that "applying prescriptive rules to information that health plans hold will not only delay processing

[8]To cover many of the persons who obtain identifiable health information from covered entities, the regulation's "business partners" provision requires that covered entities apply privacy protections to entities with whom they contract for administrative and other services. See "Requiring Safeguards by Business Partners" on p. 5.

[9]See P.L. 104-191, sec. 1173(a)(2). These transactions are those with respect to (1) health claims or equivalent encounter information, (2) health claims attachments, (3) enrollment and disenrollment in a health plan, (4) eligibility for a health plan, (5) health care payment and remittance advice, (6) health plan premium payments, (7) first report of injury, (8) health claim status, and (9) referral certification and authorization.

of claims and coverage decisions, but ultimately affect the quality and cost of care for health care consumers."

On the other hand, nine commenters suggested that HHS expand the scope of the regulations to cover more of the entities that use, disclose, generate, maintain, or receive protected health information, however defined. For example, the Workgroup on Electronic Data Interchange wrote that all entities involved in electronic exchange of individually identifiable health information should be included in the rule as health care clearinghouses. Some respondents specifically remarked that the definition of "health plan" needed to be broadened so that the same rules apply to other types of insurers, such as life, disability, workers' compensation, automobile, and property-casualty insurers. According to the National Association of Insurance Commissioners, in creating their Health Information Privacy Model Act, they concluded it was "illogical to apply one set of rules to health insurance carriers but different rules, or no rules, to other carriers that were using the same type of information." However, the Health Insurance Association of America commented that health plans should not include long-term care, disability, or dental insurance because applying the rule to these products may exceed the scope of the Secretary's authorization under HIPAA.

Providers and patient rights advocates mentioned several other individuals and organizations they believe should be covered by the rule, including employers, public health officials, marketing firms, and researchers. The American Medical Association contended that such secondary users are the ones who are most likely to wrongfully disclose and misuse protected health information. In contrast, a significant number of plans, employers, and research and pharmaceutical groups thought the covered entity definitions needed to be narrowed so that certain individuals and organizations—which could include these commenters or affiliates of these commenters—would not be subject to the rule. These commenters were generally concerned that the covered entity definitions, if broadly construed, could place unnecessary burdens and costs on their activities. For example, three of these stakeholders opposed a covered entity definition that would include biotechnology companies or manufacturers that provide product support services, conduct patient assistance programs, or conduct postmarket surveillance. According to Genentech, Inc., "Congress did not intend that we or any other biotechnology company whose mission is discovering and marketing new drugs would be a 'covered entity' under [HIPAA]."

Finally, the term "entity" was found to be somewhat ambiguous, with some advocacy groups asking how the general rule would apply to

"mixed" organizations. This is an important issue because protected health information can flow between the health component and the nonhealth component of such organizations. Several stakeholders proposed that even if an organization is not a covered entity, components within the organization that fit the definition of a covered entity should be subject to the regulations. Examples provided by the AFL-CIO and the American Civil Liberties Union included on-site health clinics operated by an employer, and a school nurse who is employed by or under contract with a school or school system.

Business Partner Contracts

Because HIPAA authorized HHS to regulate the practices of only three entities—health plans, health care providers, and health care clearinghouses—HHS developed the concept of "business partners" as a way of providing privacy protection to identifiable information obtained by other organizations in the course of performing business functions on behalf of covered entities. Support for this provision focused on its perceived necessity—otherwise much identifiable health information would have limited privacy protection—while criticism highlighted the burden of negotiating and administering thousands of different contracts.

The business partner concept generated vociferous opposition from many of the organizations commenting on the proposed rule. Eight groups including health plans and employers as well as physicians urged that HHS drop this approach altogether. Two patient rights groups plus the National Association of Attorneys General expressed support for the business partner section as written in the proposed rule.

Many of the stakeholders opposed to this provision argued that it would result in a vast number of contractual relationships that would be both costly and burdensome to implement. The Joint Commission for the Accreditation of Healthcare Organizations, for example, estimated that it would have to enter into approximately 20,000 separate contracts if it was forced to operate as a business partner in accrediting health care providers. Several commenters also maintained that the Secretary of Health and Human Services lacks the authority to indirectly extend the scope of privacy protections beyond the covered entities designated in HIPAA.

Over half of the commenters provided suggestions intended to make the application to business partners less onerous. The single most frequent recommendation, endorsed by 12 of the 31 groups commenting on this section of the proposed rule, would exempt covered entities from the definition of "business partner." The logic underlying this suggestion is

that any group that was a covered entity was already obligated to protect the privacy of identifiable health information, making business partner contracts between covered entities unnecessary. Similarly, the Joint Commission and the National Committee on Quality Assurance argued that accrediting organizations such as themselves act as health oversight agencies on behalf of government programs and therefore should not be treated as business partners.

A second major area of concern among stakeholders commenting on this section involved the degree to which covered entities would be expected to monitor the compliance of their business partners with their contractual obligations. Some sought to weaken the language of the proposed rule, which would hold the covered entities responsible when they "knew or reasonably should have known" about privacy violations committed by their business partners and failed to act. Eleven organizations including health plans, employers, and providers supported the view that covered entities should not be responsible for the actions of their business partners at all, or at most just for those violations that they actually knew about. By contrast, the National Association of Attorneys General specifically endorsed the idea that covered entities should routinely monitor the compliance of their business partners.

Finally, there was widespread opposition among six of the eight stakeholder categories to the requirement in the proposed rule that business partner contracts include a provision stating that the individuals whose identifiable information was disclosed were "third party beneficiaries of the contract." This was generally presumed to provide individuals whose privacy was violated in some way a basis for a "private right of action," allowing them to file a lawsuit. Such recourse is not provided in HIPAA directly, and 18 different commenters took exception to this apparent effort to achieve that goal through business partner contracts.

Standing Authorization for Disclosures for Treatment, Payment, and Health Care Operations

A central element of the proposed rule is to move away from requiring patients to consent to sharing their identifiable health information in order to have their health care services paid by a third party. Instead, the rule would grant standing authority to health plans, health care providers, and health care clearinghouses to share this information as they perform their routine tasks in administering health care services. In fact, the rule would prohibit covered entities from requesting such authorization unless it was required by state or other applicable law. Many of the commenters endorsed this shift to standing authorization for such routine administrative purposes, including organizations representing providers,

accrediting agencies, researchers, and health plans. Fourteen groups agreed that providers and health plans should be allowed to obtain patient consent for these purposes. They found the process of obtaining consent was useful for maintaining trust and keeping patients informed even if it was not legally required.

The main controversies involving this section concern the scope of activities encompassed by the terms "treatment," "payment," and "health care operations." Several patient rights and provider groups felt that these terms were defined too broadly. For example, the Georgetown University Health Privacy Project requested that the definitions of treatment and payment be narrowly construed as applying only to the individual who is the subject of the information.[10] The Health Privacy Project and others also argued that many health care administrative tasks could be performed without using identifiable health data. There was also a general wariness of administrative activities that could serve other purposes, such as marketing.

By contrast, most health plans and employers pressed HHS to expand its definition of treatment, payment, and health care operations so as to explicitly include such activities as disease and risk management, health promotion, quality improvement and outcomes evaluation, cost-effectiveness reviews, and integrated health and disability programs. Many insurers wanted explicit inclusion of underwriting and fraud prevention and investigation. Several commenters maintained that efforts to improve quality of care and promote innovation in health care could suffer if the definition of health care operations means that providers and health plans could not readily take advantage of the identifiable health data needed for these initiatives.

Some argued that HHS should not even attempt to enumerate the tasks encompassed by treatment, payment, and health care operations because such tasks were both highly varied and prone to change over time as innovations in health care delivery occurred. "Every time we speak with our members regarding this regulation," noted the American Hospital Association, "we discover another unanticipated, but legitimate, use of information. We cannot foresee all possible legitimate and necessary uses of information any better than HHS staff." Some commenters recommended, as an alternative to an exhaustive list, a more general

[10]The Health Privacy Project claimed that many people "would be mortified to learn that their health information was being reviewed for the treatment of others–particularly people they know."

authorization to share data reasonably related to treatment, payment, and health care operations.

Minimum Necessary Information

HHS proposed that covered entities be prohibited from using or disclosing more than the minimum amount of protected information necessary to accomplish the intended purpose of the disclosure (taking into consideration practical and technological limitations and costs). With certain exceptions, covered entities would be required to take steps to limit the amount of information disclosed from a record to the information needed by the recipient for a specific purpose.

Thirty-four of the 40 selected organizations commented on this topic, and 13 of them—representing every category of stakeholder—indicated support for the provision as written or with modifications. Healtheon/WebMD was particularly supportive, saying the requirement "will encourage better system design, attention to access controls, and more thoughtful transmission of data with a resultant improvement in privacy protection."

Another nine commenters, including providers, research organizations, and health plans, called for substantial modification of the standard, or that it be deleted from the rule entirely. These stakeholders generally believed that the "minimum necessary" standard is unworkable in its current form. Moreover, six groups, mostly those associated with employers and health plans, found the provision excessively burdensome or costly to implement.

The comment most often made on this section was that the exclusion of important clinical information could adversely affect patient care. Concerned that the standard would hinder the free flow of critical medical information, letters from several stakeholders suggested that the minimum necessary requirement not be applied to disclosures related to treatment. As the American Hospital Association put it, "what may appear unnecessary from the lab technician's or nurse's perspective may be essential for the physician's diagnosis of the patient's condition. This subjective standard could encourage practitioners in hospitals to withhold information hundreds and thousands of times daily that could be essential for later care."

Various groups wrote that the limited exceptions to the standard be broadened. For example, the Association of American Medical Colleges believed disclosures for education should be excluded from the requirement. The Department of Justice and the National Association of Attorneys General asserted that the minimum necessary rule should not

apply to disclosures to health oversight agencies and law enforcement agencies, or to disclosures needed to process applications for government benefit programs. The American Council of Life Insurers stated that the standard should not apply to insurers requesting protected information for underwriting applications or evaluating claims.

Several other groups held a contrary position: the minimum necessary provision should apply to all or most uses and disclosures of individually identifiable health information, including those for law enforcement, research, and health oversight purposes. These stakeholders believed that the exceptions in the regulation are too broad. For example, the Health Privacy Project and the American Civil Liberties Union wanted the standard to apply even when an individual requests the covered entity to disclose his or her own records.[11] Similarly, Healtheon/WebMD thought the minimum necessary standard should apply to all uses and disclosures permitted under the regulation, including those required by law.[12]

A significant number of commenters suggested that HHS create a clear definition of the term "minimum necessary." Several found the standard ambiguous and were uncertain how the requirement that only the "minimum amount of protected health information necessary" be used or disclosed should be applied. Guidance from HHS was requested by some stakeholders regarding how to make minimum necessary determinations. A few stakeholders are particularly concerned about how these provisions apply to protected health information transmitted to health plans and employers. Quintiles Transnational wrote that "the definition of 'minimum necessary' is highly subjective and no bright line test or guidance is in the regulation as to how this requirement can be met." Merck-Medco Managed Care expressed concern that organizations would be put in "a position where HHS makes an after-the-fact decision on whether [the organization's determination] on the amount of information to disclose was appropriate."

Stakeholders noted that because information requests are often vague and do not specifically contain the intended use of the information, covered entities may have difficulty determining which health information is appropriate to release. Nine commenters suggested that covered entities be allowed to apply general guidelines rather than make individual determinations. Researchers in particular believed a "good faith" guideline

[11]Excepted at sec. 164.506(b)(1)(i).

[12]Excepted at sec. 164.506(b)(1)(ii).

should be applied in enforcing the standard. This is because, as elaborated on by Genentech, "in marked contrast to the reasonableness and 'scalability' discussed in the preamble, the only flexibility in applying this standard is prosecutorial discretion."

Several other stakeholders echoed a need for flexibility in the implementation of this standard, particularly for uses and disclosures within a covered entity. For example, the American Medical Informatics Association proposed that "covered entities that use safeguard mechanisms within [computerized patient record] systems should be deemed in compliance with the 'minimum necessary' requirement." The Workgroup on Electronic Data Interchange wrote that covered entities should be "free to implement [the standard] as they see best" and "would need only to 'reasonably determine' the minimum necessary data to share within a covered entity."

Another approach to addressing the implementation problem, offered by several stakeholders across the spectrum, was to require that that the person requesting the information make a "minimum necessary demand." Patient advocacy groups noted that this would be appropriate when the disclosing covered entity does not have the ability to determine the minimum amount necessary. As stated by the Medical Group Management Association, "it is likely that the entity requesting information for a particular purpose is in a better position to make the minimum necessary determination."

Individual Authorizations

Traditionally, uses and disclosures of identifiable health information were supposed to take place only with the authorization of the individual involved. However, such authorizations frequently took the form of a "blanket authorization" that the patient had to sign in order to obtain access to and payment for treatment. The proposed rule would fundamentally alter that approach by permitting health plans, health care providers, and health care clearinghouses to share personally identifiable health data without authorization from the patient for purposes of providing and paying for health care services. The rule would give other entities access to such information without individual authorization for specific purposes related to "key national health care priorities." These activities include public health activities, health care oversight, and maintenance of governmental health data systems. Comparable access would also be granted to promote several additional nonhealth-related priorities, such as banking, law enforcement, and judicial and administrative processes.

For every other purpose, the proposed rule mandates individual authorizations that conform with strict procedural requirements. These other purposes represent, for the most part, nonhealth-related activities, such as marketing and fundraising. In addition, the rule specifies that psychotherapy notes should not be disclosed without authorization in the course of routinely administering health care delivery and reimbursement (though they are not shielded from disclosure without authorization for any of the national priority purposes). The prohibition on disclosure without authorization would also apply for "research information unrelated to treatment," which the rule defines as information developed in the course of conducting research that does not have validity or utility for purposes of providing treatment, given existing scientific evidence.

There were widely scattered comments on various aspects of these procedural requirements. Among those receiving the widest support was the provision that health plans and providers should not be able to refuse treatment or payment because a patient had declined to authorize disclosure of their identifiable health information for other purposes. However, BlueCross BlueShield requested that health plans be allowed to condition enrollment on the provision of individual authorization for disclosure of psychotherapy notes. There was also support among patient rights groups, physicians, and state attorneys general for preventing uses and disclosures beyond those authorized by the individual.

Other comments had more to do with defining the types of health data for which individual authorization would be required. Nine commenters found the rule's definition of "research information unrelated to treatment" vague or ambiguous, and six recommended that HHS drop this separate category of health data altogether. These commenters were primarily health plans, employers, or groups representing medical researchers. According to the Biotechnology Industry Organization, "providers anticipate daily struggles in deciding whether information resulting from participation in a research protocol should be included in a patient's medical record (in case such information becomes critical to a patient's treatment at a later date) or whether such information should be excluded from the medical record to avoid civil and criminal penalties." This statement was typical of the concern expressed by these groups toward this special category of identifiable health information.

In contrast, two patient advocacy groups sought to ensure that once information was classified as "research information unrelated to treatment" it could not be reclassified at a later date. In addition, privacy advocacy groups sought stronger protection for "psychotherapy notes," while comments from a few health plans sought to limit the special

treatment that the rule would afford this category of identifiable health information.

A related topic of widespread interest was disclosure of protected health information for "marketing" purposes. Several stakeholders called on the Secretary to define this term. Three health plans and four other stakeholders did not support requiring authorization for health-related activities, even if they had a business connection, such as reminders to refill prescriptions. On the other hand, the National Association of Attorneys General would prohibit all disclosures for marketing even with individual authorization.

Several commenters expressed a comparable concern about disclosures for employment purposes. The AFL-CIO wrote that employees should be clearly informed that they have the right to refuse to authorize disclosures without penalty. A similar concern, expressed by three patient rights groups, was that employers not have the right, without the authorization of the individual involved, to share identifiable health information between divisions within the organization that functioned as health plans or providers and the rest of the company. However, two employer groups and one health plan said that sharing of identifiable information within a covered entity without authorization should be allowed.

Finally, some of the patient advocacy groups recommended that the rule extend heightened protection for another category of health data. For example, the Bazelon Center for Mental Health Law took the position that "the rule should create a special category of highly sensitive medical information provided higher levels of privacy protection, e.g. HIV status and mental illness." However, other stakeholders said there should be no special treatment for different illnesses or categories of health information. For example, the American Health Information Management Association believed that such segregation "ultimately would be more dangerous than beneficial."

Some Modifications May Require Action by the Congress

In its preamble to the rule, HHS explicitly noted that HIPAA set limits on its authority to apply privacy protections comprehensively and uniformly. Many commenters cited a need for the Congress to act if personal health information is to be subject to the same standards regardless of how it is stored (exempting purely paper records) or where the individual resides (excepting more stringent state laws). Still, stakeholders often disagreed on the steps the Congress should take to make the proposed regulation optimal or workable.

The most frequent suggestion was that the Congress enact a uniform federal medical records privacy law that would preempt all state laws. Three employers and three health plans stressed the need to eliminate any variation in standards, but no patient rights groups or government stakeholders offered this suggestion. One clearinghouse said that it strongly believes that "federal health information standards must preempt the patchwork of inconsistent State requirements if they are to provide real assurances of privacy to individuals at a time when health care is increasingly an inter-State enterprise."

Many stakeholders also called for legislative modification to the "applicability" section of the regulation. Some proposed that the Congress extend HHS' authority to cover all identifiable health information, regardless of whether it had ever been electronically stored or transmitted, even though HHS declared in the proposed rule that under current law it could have chosen to do so. A substantially larger group of commenters from across the spectrum of stakeholder categories advocated legislative changes to extend coverage under the rule to all types of entities that use or disclose identifiable health information. Perhaps anticipating this argument, the American Hospital Association wrote that "the reason Congress limited the applicability of the Secretary's regulations to these [nine] transactions is that: (1) the public was concerned about inappropriate disclosures between payers and providers, and (2) these were the transactions made more administratively efficient by HIPAA, which may heighten those concerns. … [The Secretary's] broad interpretation of statutory intent is the 'Achilles heel' of this regulation."

A need for congressional action was also cited in comments on various other sections of the regulation, primarily to limit secondary uses or disclosures of identifiable health information. A number of stakeholders asked for comprehensive privacy legislation to cover other areas as well as health. Regarding enforcement, three stakeholders stated that the Congress should establish a private right of action for individuals to enforce their rights under the privacy rules. A patient advocacy group went further in asking for the Congress to recognize a patient's ownership of his or her medical records. Some stakeholders explicitly noted that only legislation could enable the Secretary to directly regulate noncovered health researchers.

Concluding Observations

The comments that we reviewed from major organizations—representing many of the entities that will have to implement the policies adopted—reflected two overriding themes. The first is a widespread acknowledgement, despite the organizations' diverse perspectives, of the

importance of protecting the privacy of medical records. While the groups may vary in their assessment of the best way to achieve that goal, none challenged its fundamental value. Second, fundamental differences among the groups' positions reflect the conflicts that sometimes arise between privacy and other objectives. Different groups with varying constituencies tended to emphasize different competing goals. As HHS considers the comments in formulating the final rule, it will have to make its own judgments regarding both the relative priority to give to other objectives and the merit of differing views on the feasibility of alternative approaches for protecting medical privacy. These judgments will occur within the context of what the law currently permits and requires, unless the Congress decides to change the statutory framework established by HIPAA and related federal legislation.

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 Janet Heinrich, Associate Director, Health Financing and Public Health Issues, at (202) 512-7119. Other individuals who made contributions to this statement include Barry Bedrick, Robert Crystal, Rosamond Katz, Eric Peterson, Daniel Schwimer, Victoria Smith, and Craig Winslow.

Selected Stakeholders in the Debate Regarding Federal Health Privacy Policy

We included the following organizations' comments in our review:

AFL-CIO
American Association of Health Plans
American Association of Retired Persons
American Civil Liberties Union
American Council of Life Insurers
American Health Information Management Association
American Hospital Association
American Medical Association
American Medical Informatics Association
American Psychiatric Association
American Psychological Association
Association of American Medical Colleges
Association of Private Pension and Welfare Plans
Bazelon Center for Mental Health Law
Biotechnology Industry Organization
Blue Cross Blue Shield Association
Genentech, Inc.
Georgetown University Health Privacy Project
Health Insurance Association of America
Healthcare Leadership Council
Healtheon/WebMD
Intermountain Health Care
Joint Commission on Accreditation of Healthcare Organizations
Medical Group Management Association
Merck-Medco Managed Care, L.L.C.
National Association of Attorneys General
National Association of Insurance Commissioners
National Breast Cancer Coalition
National Committee for Quality Assurance
National Committee on Vital and Health Statistics
National Conference of State Legislatures
National Governors' Association
National Uniform Billing Committee
National Uniform Claim Committee
Pharmaceutical Research and Manufacturers of America
Quintiles Transnational
U.S. Department of Justice
UnitedHealth Group
Washington Business Group on Health
Workgroup on Electronic Data Interchange

(201015)

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 (automated answering system)