

February 25, 2000

Margaret A. Hamburg, MD
Assistant Secretary for Planning and Evaluation
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Re: Small Business Impact: Comments on the proposed Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,917 (November 3, 1999).

Dear Dr. Hamburg:

The Office of Advocacy of the U.S. Small Business Administration (SBA) was established by Congress under Pub. L. No. 94-305 to advocate the views of small business before federal agencies and Congress. Advocacy is also required by section 612(a) of the Regulatory Flexibility Act (RFA)¹ to monitor agency compliance with the RFA. In addition, the Chief Counsel of Advocacy is authorized to appear as *amicus curiae* in regulatory appeals from final agency actions, and is allowed to present views with respect to compliance with the RFA, the adequacy of the rulemaking record with respect to small entities, and the effect of the rule on small entities.² On March 28, 1996, President Clinton signed the Small Business Regulatory Enforcement Fairness Act (SBREFA)³ which made a number of significant changes to the RFA, including the provision to allow judicial review of agencies' compliance with the RFA.⁴

The Proposal

On November 3, 1999, the Department of Health and Human Services (HHS) proposed the above-referenced rulemaking pursuant to Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The regulations are intended to provide standards to protect the privacy of individually identifiable health information maintained or transmitted electronically. The rules apply to health plans, health care clearinghouses, and most health care providers. Specifically, the rule addresses the rights individuals have with regard to their medical records, and the authorized and required uses and disclosures of this information.

Although one of the goals Congress had in mind with respect to this privacy regulation was administrative simplification, the proposal is anything but simple. In fact, there are so many over-broad, unenforceable, over-complicated and over-burdensome provisions in this proposed regulation, that compliance would be virtually impossible for even sophisticated business operations. Granted, many of the fatal flaws in the proposal exist

¹ 5 U.S.C. § 601 et seq.

² *Id.*

³ Pub. L. No. 104-121, 110 Stat. 857 (1996).

⁴ 5 U.S.C. § 6111.

because of the limited Congressional authority granted to HHS in drafting the regulation. However, a lot of the flaws are due to HHS' own design. HCFA took on a gargantuan task—a task that Congress could not manage prior to expiration of the statutory deadline for congressional action on the issue. Unfortunately, HHS' effort has resulted in little more than regulatory micro management. Even though HHS has made an attempt to make the regulation flexible and scaleable for different sized businesses so as to reduce burden on smaller entities, the facts are that businesses (particularly small practitioners) will be burdened, patient privacy will not be adequately protected and the administrative simplicity contemplated in HIPAA will not be attained.

This comment letter will address some of the bigger problems associated with the proposal, and in so doing, will focus primarily on small practitioner burden. The Office of Advocacy had hoped that some of the issues raised herein would have been addressed prior to publication of the proposal, as discussed in meetings with HHS and OMB staff. However, it seems that a number of the problems that Advocacy cited in the draft proposal remain and still need to be addressed or explained by HHS. The Office of Advocacy concludes now, as it did during the draft phase of the rulemaking, that the proposal is too problematic to move forward—unless significant changes are made.

The Secretary's Authority to Regulate Business Partners

The Secretary's authority to promulgate this privacy regulation comes from HIPAA. According to section 1172 of HIPAA, the rule is only applicable to health plans, health care clearinghouses, and health care providers who transmit health information in electronic form. This scheme leaves a big loophole because the statute does not grant the authority to cover directly many of the persons or entities that obtain identifiable health information from covered entities (e.g., billing contractors, lawyers, insurance companies, etc.). To close the loophole, HHS has proposed to regulate non-covered entities indirectly. HHS states, "We would attempt to fill this gap in our legislative authority in part by requiring covered entities to apply many of the provisions of rule to the entities with whom they contract for administrative and other services [i.e., 'business partners']."⁵

The Office of Advocacy does not believe that the Secretary has the legal authority to regulate—directly or indirectly—entities that are not covered under HIPAA. The plain language of the statute reveals that Congress intended for HHS to regulate only those types of entities listed in HIPAA. Moreover, Advocacy is not aware of any other general authority that the Secretary may have to expand the definition of a covered entity in this rulemaking. Since Congress did not intend for HHS to regulate business partners, HHS' attempts to reign in business partners indirectly could be considered as arbitrary and capricious.⁶

⁵ 64 Fed. Reg. at 59,924.

⁶ Whether or not an agency action is arbitrary and capricious is determined by the following test: "**if the agency has relied on factors which Congress has not intended it to consider**, entirely failed to consider an important aspect of the problem, offered an explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of

The proposed rule requires the various providers of health care to monitor/police the compliance of their “business partners” with the privacy standards. Moreover, section 164.518(f) of the proposal requires covered entities to mitigate the damages caused by a business partner that violates the privacy standards. However, the penalties (civil and criminal) that apply to covered entities for divulging individually identifiable health information do not apply to business partners. Therefore, the covered entity will be held responsible for uncontrollable acts of its business partners, but no such accountability attaches to the business partners. This unfair and confounding result basically stems from the fact that HHS has no authority to regulate business partners.

It is not even clear how the business partner relationship could work in the real world. Many different physicians may have privileges at many different hospitals. Which is the covered entity—the hospital or the physician? How can a hospital monitor all physicians who use their hospital and vice versa? The economic impact of forcing covered entities to police their business partners is another matter of concern; however, the issue of impact will be discussed elsewhere in these comments. Clearly, the regulation of business partners should be left to Congress, and HHS should abandon its attempts to make law.⁷

Confusing Concepts

There are a number of confusing concepts in the instant proposal that make compliance extremely difficult. If the regulated entities cannot comply, then the regulation will be useless in protecting privacy. Moreover, entities attempting to comply with ambiguous or over broad provisions might incur unnecessary additional costs in trying to decipher the regulation or in legal actions to force clarification.

Mixed Records

Since only electronic records are covered under HIPAA, HHS is proposing that certain records be designated as “mixed records” (i.e., containing both protected and unprotected information). Providers would have to devise a way to insure that electronic records meet the privacy standards when mixed with unprotected paper records. There does not appear to be any feasible way in which to manage this task because electronic records can be printed, and records that started out in paper form could have been entered into a computer at some point and re-printed. Keeping two sets of records would be infeasible as well. HHS’ suggestion to identify one set of records with a watermark would likely have a low level of reliability, and therefore, would not be feasible either.

agency expertise.” Emphasis added. *Motor Vehicle Manufacturers Association v. State Farm Mutual Automobile Insurance, Co.*, 463 U.S. 29, 43, 103 S.Ct. 2856, 2866 (1983).

⁷ The rulemaking power granted to an agency charged with administration of a federal statute is not the power to make law. Rather, it is “the power to adopt regulations to carry into effect the will of Congress as expressed by the statute.” *Ernst & Ernst v. Hochfelder*, 425 U.S. 185, 213-14, 96 S.Ct. 1375, 1391 (1976).

Advocacy does not have any suggestions that would make the task of managing mixed records easier. The simplest way to deal with the situation would be to require that all records meet the same privacy standards. This solution would certainly provide a greater level of reliability and enforceability, however, Advocacy is not aware of whether the Secretary has the authority to bring unprotected paper records under the scope of this regulation.

Minimum Necessary

A central aspect of the proposal is the principle of “minimum necessary” disclosure. According to HHS, “With certain exceptions, permitted uses and disclosures of protected health information would be restricted to the minimum amount of information necessary to accomplish the purpose for which the information is used or disclosed . . .”⁸ Using this principle, each time a request for information is made, health providers would have to make a new determination as to what the minimum necessary information is for that particular requester (e.g., an employer, law enforcement, a relative, etc.). This standard seems terribly subjective. Moreover, it puts the health provider in the untenable position of having to figure out whether that particular individual actually needs certain requested information.

Advocacy’s criticism of this principle should not be misconstrued to mean that minimum necessary disclosure is not a valid concept. For instance, a lawyer investigating a personal injury claim might need to see the medical records connected with injuries received in an accident, but that lawyer would have no need to see the injured person’s entire medical record on childhood vaccinations or previous surgeries. On the other hand, the lawyer might need information about an epileptic condition that may have contributed to the accident. The point is that it is impossible for the health provider to know what the minimum necessary disclosure is without violating an individual’s privacy. HHS must devise a way to take the burden off of the health provider.

De-identifying Information

De-identified information is patient information that has been stripped of nineteen designated characteristics, including the patient’s name, medical record number, etc. HHS is proposing that covered entities and their business partners be permitted to use protected health information to create de-identified health information. Covered entities would further be permitted to use and disclose such de-identified information in any way, provided that they do not disclose the key or other mechanism that would enable the information to be re-identified.

However, in addition to removing the nineteen characteristics, section 164.506(d)(2)(ii)(B) of the regulation requires health providers to determine whether “any anticipated recipient of such information could use the information, alone or in combination with other information, to identify an individual.” HHS should not require health providers to speculate about potential or unknown recipients and whether those

⁸ 64 Fed. Reg. at 59,924.

unknown recipients possess information that could re-identify the information. Removing this provision would make compliance easier.

Federal Preemption

These regulations will pre-empt all less stringent state laws on medical record privacy. However, more stringent state laws will be allowed to prevail. Understandably, there are important states' rights concerns imbedded in the issue of preemption. Advocacy believes that the Secretary recognizes the statutorily imposed limitations of this proposal and, therefore, is allowing more stringent state laws to remain in effect. Nevertheless, this creates a quagmire of different laws to which covered entities must adhere—a compliance jungle.

In this compliance jungle, no guidance is offered to assist covered entities in determining how their particular state laws would compare with the federal requirements. More importantly, there is no guidance or process for covered entities to seek guidance from the federal government on how to comply when there is a potential conflict. Of course, states can request a determination from HHS when there is a conflict, but covered entities cannot do so directly. It is difficult to imagine what this process—or lack of process—could do to the business operations of a small practitioner.

HHS should make some effort to design a more manageable process.

Underestimated Burden

HHS estimates that the rule will cost between \$1.8 billion and \$6.3 billion over five years, but these estimates do not consider all of the costs imposed by the regulation. Advocacy believes that these estimates are extremely low and are based on weak and unsupported assumptions.

Failure to Include Major Costs in Estimates

As noted in the preamble, HHS did not consider a number of significant costs imposed by the regulation:

“ In some areas . . . there was too little data to support quantitative estimates. As a result, the RIA does not include cost estimates for all of the requirements of the regulation. The areas for which explicit cost estimates have not be [sic] made are: The principle of minimum necessary disclosure; the requirement that entities monitor business partners with whom they share PHI; creation of de-identified information; internal complaint processes; sanctions; compliance and enforcement; the designation of a privacy official and creation of a privacy board; and additional requirements on research/optional disclosures that will be imposed by the regulation. The cost of some of these provisions may be significant, but it would be inaccurate to project costs for these

requirements given the fact that several of these concepts are new to the industry.”⁹

Most of the estimates provided by HHS are entirely assumption based, so it does not seem possible that HHS could not provide even a range of estimates for some of these significant requirements.

In addition to providing little if any quantification for the requirements listed above, there are a number of effects related to these unquantifiable requirements that have not been adequately described in a qualitative fashion. For instance, the fact that business partner contracts may have to be renegotiated and not simply rewritten has not been addressed. Moreover, in some cases, contract prices might increase, or additional liability insurance may be required due to the additional liability associated with the business partner monitoring requirement.

Aside from the costs that HHS identified, but could not calculate, there are other new requirements that will impose costs on the industry that HHS did not identify at all. There is no analysis, for instance, to assist covered entities in determining the costs associated with deciphering whether the federal law preempts the state law. Also, HHS assumes that national and state associations representing the regulated industries will develop privacy policies and procedures for adoption by individual member entities. However, HHS is ducking its responsibility for evaluating the cost by assuming that an unregulated third party will assume the cost. Section 607 of the RFA requires agencies to provide either a quantifiable or numerical description of the effects of a proposed rule or alternatives to the proposed rule, or more general descriptive statements if quantification is not practicable or reliable.

Cost Estimates Lack Justification

Most of the cost estimates that do appear in the proposal are either not explained or are based on assumptions that are not explained. The analysis of initial costs is discussed below in the order in which they appear in the regulation:

- Assuming that the requirements for developing formal processes and documentation of procedures mirror what will already have been required under the earlier security regulations, and assuming that associations will develop guidelines for use by their members (apparently, at no cost to the associations), HHS estimates that providers will incur a range of costs from \$300 to \$3000, with a weighted average of \$375 per entity. The aggregate cost of establishing policies and procedures is estimated to be \$300 million. The Office of Advocacy can find no support for these estimates in the regulation. Moreover, the estimates seem unreasonably low inasmuch as Advocacy has identified scores of new procedures and requirements in the proposal (e.g., new business partner contracts, new disclosure policies, initial and ongoing training for every worker and practitioner, new business partner monitoring obligations, etc.).

⁹ 64 Fed. Reg. at 60,015.

- With respect to revisions and upgrades to computers, HHS concludes the overall administrative simplification system upgrades in HIPAA of \$5.8 billion would be disproportionately associated with the previously proposed security standard relative to the other elements. Then, HHS assumes that if it constitutes fifteen percent in privacy, then the security standard would represent about \$900 million system costs. Then, HHS assumes that if the marginal cost of the privacy elements were another ten percent, then the additional cost would be \$90 million. Frankly, the logic of this entire “analysis” eludes Advocacy. What is the basis of the ten and fifteen percent assumptions?
- The requirement of providing patients a notice regarding their privacy rights is estimated to cost between \$300 and \$3000 per provider. The total development cost for new notices is estimated at \$30 million over five years, and the cost of providing notices to patients and providers is supposed to be \$106 million for the first year and \$209 million over 5 years. These figures are based on some assumed number of patients (543 million) and on the assumption that these patients will visit some sort of health provider at least once during a 5-year period. The patient estimate is based on a 1996 survey that provides the number of episodes and encounters of care per year for hospitals, home health agencies, etc. The patient estimate is also based on the unsubstantiated assumption that an additional 25% of the remaining population will enter the system, and thus receive the notice. For obvious reasons, an episode is not a patient—patients can have multiple episodes. Without a valid patient count, the cost estimate for the notice requirement is useless. At any rate, the requirement that the notice be provided every three years is unnecessary unless there has been some change in the provider’s privacy policies. Removing this requirement would help reduce the cost—whatever the true cost really is.

HHS also states that most health plans will provide an independent mailing the first year pursuant to the notice requirements in the regulation, but would include notices with other mailings in subsequent years. The five-year cost of this little exercise is estimated at \$0.75, with a total cost for all entities at \$231 million over five years. A stamp the first year would cost \$0.33, so \$0.42 is left to cover all administrative, printing/copying, personnel and supply costs. How is this possible?

- On inspection and copying, HHS estimates that 1.5 percent of patients will request access to inspect and copy their medical records, and that the cost of accessing and copying a record is about \$10. While the cost of copying is based on a Tennessee study, the percentage of patients requesting records appears to be a guess. The Office of Advocacy has not seen this Tennessee study, therefore it is not known whether higher regional wage costs were taken into account. Moreover, the estimate seems a bit low when one considers that even a minimum wage employee earns over \$5 per hour.
- Under the proposal, individuals have the right to request amendment and correction of their medical records. HHS estimates that there will be an average cost of \$75 per

instance. What is the basis of this figure? Using the \$75 estimate and two-thirds of the assumed number of patients that will be requesting inspection and/or copying, the agency estimates that the total cost will be \$407 million annually, or \$2 billion over five years. What is the basis for the number of patients requesting amendment or correction?

- In some instances, patient authorizations will be needed before records can be released. HHS estimates that one percent of encounters will require obtaining such authorizations. The basis of this estimate cannot be discerned from the rule.
- Regarding paperwork and training, HHS assumes a cost of about \$20 per provider office, and \$60-\$100 for health plans and hospitals. The total cost of paperwork and training is estimated at \$22 million per year. \$20 for training? Where did this come from? HHS assumes that training happens as a regular business practice and that the marginal costs of the new training requirements will therefore be low. Perhaps costs will be lower in the out years when polices have been in effect for a while; but initially, doctors, nurses, hospital staff, and many other health professionals will experience a huge learning curve. This training estimate is way too low.
- Finally, HHS makes no true attempt to quantify future costs beyond five years. HHS simply states that “Future costs beyond the five year period will continue but will not be as great as the initial compliance costs.”¹⁰ Aside from drafting and renegotiating new business partner contracts and drafting the new policies and procedures, the majority of the costs associated with this regulation are ongoing in perpetuity—the training, the paperwork and record keeping, the business partner monitoring, etc. It is not adequate to simply dismiss the tremendous future costs of this regulation by stating that they will not be as great.

Benefits are Speculative

The benefits analysis in the proposal is actually less clear than the cost analysis described in the previous section of this comment. HHS tries to use a qualitative and quantitative measure of benefits in the proposal. Qualitatively speaking, HHS claims that a well designed privacy standard will build confidence among the public about the confidentiality of their medical records. This new confidence will result in increased utilization of health care, which will result in screening and early detection of health problems, and more successful treatment. Early detection of cancer or HIV/AIDS, for instance, will prolong survival or reduce costly disability. Quite a bit of data is presented on the cost of various types of illnesses--\$104 billion for cancer (including medical, morbidity and mortality costs). However, translating these costs into benefits requires a bit of a stretch. In the case of mental illness, HHS states that a reasonable upper limit of the number of individuals avoiding mental health treatment for fear of having their condition revealed might be 1.8% (or, 25% of the 7% of survey respondents that indicated they would avoid mental health treatment due to the potential adverse impact

¹⁰ 64 Fed. Reg. at 60,044.

on their jobs or other life opportunities). There is no indication of where the 25% comes from. Using the 1.8%, upper limit multiplied by the annual economic cost of mental illness (\$115.5 billion—for the four main mental disorders), and a treatment effectiveness rate of 80 percent, the annual benefits amount to \$1,039,500,000. The lower limit is calculated in a similar fashion. It took quite a bit of work to arrive at this impressive benefit/savings. It can all be easily undone, however, if one considers the likely scenario that this regulation will not be the magic pill that inspires mental patients or cancer patients to suddenly seek early medical treatment. The analysis is not credible.

In its quantitative analysis of benefits, HHS says that it has figured out a way to calculate the value an insured individual would place on increased privacy to make the proposed regulation a net benefit to those who receive health insurance. In one alternative, HHS divides the total cost of complying with the regulation, \$751 million per year, by the total annual number of health care encounters. The cost of implementing requirements of the proposed regulation, therefore, is \$0.46 per health care encounter. HHS assumes that individuals would be willing to pay more than \$0.46 to improve health information privacy, and then draws the conclusion that the benefits of the proposed regulation will outweigh the cost. In another alternative, HHS believes that it can take annual cost of the regulation and divide it by the 220 million individuals that are insured to achieve an estimated annual cost of \$3.41 per insured individual. Again, HHS assumes that individuals would be willing to pay more than \$3.41 to insure their privacy.

This type of benefit analysis is called a “willingness-to-pay” analysis. It provides an aggregate measure of what individuals are willing to forgo to enjoy a particular benefit. While such innovative analysis techniques may be useful in some cases, a general requirement is that there be a mechanism to ensure that estimates are reliable in the first place. The Office of Advocacy opines that the \$751 million figure misses the mark entirely and that any calculation based on that figure would be unreliable.

Overlapping Ethical Requirements Contribute to Unnecessary Cost

As stated throughout this comment letter, the Office of Advocacy believes that this proposal is too costly and fails to protect patient privacy adequately. If HHS were to evaluate the source of most privacy problems, it probably would not lie with the small practitioners of the world. Are pharmaceutical companies likely to obtain health information from a small practitioner or a large chain pharmacy? The point is that physicians are already ethically and legally obligated to maintain their patients’ privacy. Therefore, this confusing, unenforceable and expensive regulation merely adds to the burden of physicians. Current state laws exist that allow licensing boards to deal with physicians who violate patient confidentiality.

The scalability provisions are not sufficient to remove the excess burden associated with this regulation. Even if a practitioner does not conduct electronic record transactions, that practitioner would become subject to most of the rule’s requirements if another entity using the records transmits the information electronically.

The fact that small practitioners are already under ethical and legal obligations to protect their patients' privacy, coupled with the fact that compliance with this proposal would be nearly impossible for even sophisticated health providers, leads the Office of Advocacy to conclude that some sort of exemption for small practitioners might be appropriate. That is, an alternate scheme whereby greater reliance were placed on individual patient authorizations might be more manageable than trying to determine who has a legitimate need for the information without authorization, and how much information they should get in every instance. Extremely narrow cases could be carved out for the few instances where pre-authorization would not be required—however, HHS should avoid getting into the trap of trying to anticipate every possible use for the information. Perhaps this approach is naïve or overly simplistic, but it seems like a good baseline from which to start thinking about how a small physician's office operates.

As for all of the training, record keeping and privacy official requirements, Advocacy believes that most could be eliminated or significantly modified. In a small practitioner's office the office manager might double as the receptionist, bookkeeper and privacy official. This same person may only work on a part-time basis. In this case, having a single privacy official would not be practical. In addition, the requirement for re-certification of the privacy official every three years is not practical either. If the policies and procedures have not changed, then re-certification serves no real purpose. Finally, creating, maintaining and storing documentation of privacy policies and procedures for six years is of minimal benefit and the requirement should be made more flexible.

The RFA, Executive Order 12866, Unfunded Mandates Reform Act (UMRA),¹¹ and SBREFA

The analyses required by the above-captioned statutes and the executive order all require agencies to assess and minimize (where possible) the burden on the regulated industry. HHS clearly has made an effort within unforgiving time constraints to analyze the impact of this regulation and make some of the provisions flexible and scaleable. The problem is that most of the assumptions underlying the analysis are not supported by any evidence.

In 1996, the Office of Management and Budget (OMB) published guidelines for agencies conducting regulatory analyses pursuant to the executive order.¹² The guidelines are aimed at assuring full disclosure and transparency. In particular, OMB stated that an "economic analysis should identify and explain the data or studies on which cost estimates are based with enough detail to permit independent assessment and verification of the results."¹³ This basic axiom is true for all of the statutes requiring impact analyses.

In addition, although the RFA does not require that the least burdensome alternatives be selected, the UMRA arguably does. It states, "the agency shall identify and consider a

¹¹ Unfunded Mandates Reform Act of 1995 (Pub. L. No 104-4).

¹² Executive Office of the President, Office of Management and Budget, "Economic Analysis of Federal Regulations Under Executive Order 12866" (January 1996), reprinted in *Daily Report for Executives* (January 22, 1996).

¹³ *Id.* at M-14.

reasonable number of regulatory alternatives and from those alternatives select the least costly, most cost-effective or least burdensome alternative that achieves the objectives of the rule.”¹⁴

SBREFA requires that agencies publish compliance guidance for small businesses. Under this SBREFA requirement, agencies may prepare separate guides covering groups or classes of small businesses, and are encouraged to cooperate with associations of small entities to develop and distribute the guides.

Conclusion

Congress clearly left a number of significant loopholes in the statute, and HHS has taken on the task of filling in the blanks to try to achieve both privacy and administrative efficiency. The problem is that neither has been achieved through this proposal. When the unsubstantiated benefits of this proposal are compared to the astronomical administrative costs and burdens associated with implementation, the proposal simply makes no sense.

Advocacy urges the Secretary to withdraw the instant regulation and re-propose a new notice of proposed rulemaking that would include a more complete analysis of costs and impacts, and less complex requirements. Thank you for your consideration of these comments. Please do not hesitate to contact my office if you have any questions, 202-205-6533.

Sincerely,

Jere W. Glover
Chief Counsel for Advocacy

Shawne Carter McGibbon
Asst. Chief Counsel for Advocacy

¹⁴ Pub. L. No. 104-4, Title II, sec. 205(a).