Public Interest Comment on

The Department of Health and Human Services'

Standards for Privacy of Individually Identifiable Health Information[1]

Whatsoever things I see or hear concerning the life of men, in my attentance on the sick or even apart therefrom, which ought not be noised abroad, I will keep silence thereon, counting such things to be as sacred secrets.

— Oath of Hippocrates
4th Century BC

The Regulatory Studies Program (RSP) of the Mercatus Center at George Mason University is dedicated to advancing knowledge of regulations and their impacts on society. As part of its mission, RSP produces careful and independent analyses of agency rulemaking proposals from the perspective of the public interest. Thus, the program's comments on the Department of Health and Human Service's (HHS) proposed *Standards for Privacy of Individually Identifiable Health Information* do not represent the views of any particular affected party or special interest group, but are designed to protect the interests of American citizens. This comment extends and supersedes our comments of December 31, 1999.

I. Introduction

HHS has proposed rules to protect individually identifiable health information that is electronically stored or communicated.[2] Authority for the rule-making stems from the 1996 *Health Insurance Portability and Accountability Act*.[3] As HHS states in its proposal,

> This rule proposes a standard to protect the privacy of individually identifiable health information maintained or transmitted in connection with certain administrative and financial transactions. The rules…would apply to health plans, health care clearinghouses, and certain health care providers, propose standards with respect to the rights individuals who are the subject of this

[1] Prepared by Jay Cochran, III, Research Fellow, Regulatory Studies Program, Mercatus Center, George Mason University, jcochra1@gmu.edu.

[2] "Standards for Privacy of Individually Identifiable Health Information; Proposed Rule," 45 CFR Parts 160 Through 164. As found in the *Federal Register*, Vol. 64, No. 212, Wednesday, November 3, 1999, pp. 59918—60065. Hereinafter referred to as the "Proposed Rule." The proposed rule covers only electronic information. Paper records that have never been in electronic form would not be subject to the proposed rule's requirements.

[3] Public Law 104-191, *Health Insurance Portability and Accountability Act*, enacted August 21, 1996.

> information should have, procedures for the exercise of those rights, and the authorized and required uses and disclosures of this information.[4]

HHS identifies a growing threat to patient privacy stemming from the increased usage of electronic systems by health care providers and plan administrators to collect, process, and distribute patient information. In proposing the rule, the Department attempts to strike a balance between the need for this information to provide efficient delivery of health care and related services, and the rights of patients to have this information remain private. HHS worries however, that erosion of medical records privacy may damage public health in the long run as patients, who fear having that confidentiality violated, take steps to avoid that possibility by delaying treatment or refusing it altogether.

The rule seeks to protect individuals from encroachment by other individuals and firms on their private health records to an extent. For instance, under the rule, health care providers cannot arbitrarily disclose patient information to unauthorized parties without the patient's written consent.[5] Pharmaceutical manufacturers, to cite one example, may not cull hospital patient records without the individuals' consent to conduct biomedical research.[6] Beyond the three principal exceptions,[7] health care plans,[8] may not disclose individually identifiable health information to others.

The rule also attempts to make patient consent voluntary, informed, and revocable. Under the rule, a patient may not be denied treatment or payment on his/her behalf for failure to sign a consent form. In addition, the form itself must clearly spell out the patient's rights to privacy and the provider's obligations to respect those rights. Finally, under the rule the patient may revoke his/her consent to release protected health information at any time.

Suppliers of health care, who are covered under the rule, must take positive steps to ensure that patient records remain confidential in most circumstances. Importantly, the rule also allows the patient to take some degree of control over his/her records by allowing the patient to inspect, copy, and in some cases amend those records if he/she finds an error upon inspection. Providers and plans also may reserve the option of refusing a patient's amendment request under certain circumstances.

---

[4] Proposed Rule, p. 59918.

[5] The prohibition however, comes with myriad exceptions, caveats, and explanations, discussed below under "Strengths and Weaknesses of the Proposed Rule."

[6] Interestingly however, university and non-profit research institutions may continue to do so under the rule. The purpose for such discrimination is not clearly expressed in the proposed rule. No compelling evidence is offered to suggest that university researchers are more disposed to guard confidential information than for-profit research firms would be. HHS needs to clarify the reasons for what seems to be an arbitrary prejudice.

[7] "Under this rule, covered entities with limited exceptions would be permitted to use and disclose protected health information without individual authorization for treatment and payment purposes, and for related purposes that we have defined as health care operations." (Proposed Rule, p. 59925.)

[8] "*Health plan* means an individual or group plan that provides, or pays for the cost of, medical care." (Proposed Rule, p. 60050) This definition includes employee welfare benefit programs, health insurance companies, health maintenance organizations, and government administered plans.

II. Background

Samuel Warren and Louis Brandeis suggested more than a century ago that a right to privacy was the right to be let alone.[9] Importantly, then as now, the preservation of a right to be let alone hinged crucially on the state of technology. A century ago, advances in photography and printing gave journalists the means to invade what had previously been private domain. Today, advances in electronics and communications are lowering the cost of invading another's privacy through easy access to on-line medical, financial, and other personal information.

Historically, ownership rights have tended to go unspecified until the costs of a continued lack of specification rose sufficiently. Advances in the 19th century photography and journalism have already been mentioned. In the 20th century, air rights over land parcels went largely unspecified until the advent of modern aviation. In addition, Harold Demsetz refers to the aboriginal people of the Labrador Peninsula who held rights to indigenous game in common.[10] Game was plentiful enough that further specification of property rights would have meant costs beyond any potential benefits. The appearance of European settlers, however, changed the conditions of scarcity on Labrador such that property rights in land and game become important considerations. Similarly now, private information is at the Labradorian crossroads.

In recent information privacy cases, the US Supreme Court has ruled that the concept of "practical obscurity" effectively protects individual privacy.[11] That is, the high costs of assembling disparate pieces of information from scattered sources have allowed the individual subject of the information to remain practically obscure. However, the cost advantages of electronically storing and processing medical records have resulted in increasing volumes of medical records being stored (and accessible) on-line. Thus, the protections once afforded by practical obscurity are fading apace with the adoption of modern computers and communications in the medical field. Changing technology in other words, has once again induced the need for an elaboration of property rights, this time with respect to information.

---

[9] Warren, Samuel D., and Louis D. Brandeis (1890), "The Right to Privacy," *Harvard Law Review 5* (4), pp. 193-220. In their article, the authors trace the right to privacy—the right to be let alone—to Thomas M. Cooley's, *A Treatise on the Law of Torts*, (Chicago: Callaghan, 1880), p. 29. Thus, formal recognition of the right to privacy is at least 120 years old.

[10] Demsetz, Harold (1967), "Toward a Theory of Property Rights," *American Economic Review 57* (2), pp. 347-359.

[11] An important case is *United States Department of Justice, et. al, v. Reporters Committee for Freedom of the Press,* 489 US 749. The Court did not deal directly with the privacy of medical records, but rather limited journalists' *Freedom of Information Act* access to government "rap" sheets collected on suspects and criminals from a variety of obscure sources. "When the subject of such a rap sheet is a private citizen and when the information is in the Government's control as a compilation, rather than as a record of 'what the government is up to,' the privacy interest…is…at it apex while the…public interest in disclosure is at its nadir." (p. 780).

Putting the matter in economic terms, the cost of potentially invading another person's medical privacy (or financial, or personal privacy for that matter) has fallen as advances in technology have risen. Other things being equal therefore, we would expect a rise in the number of privacy intrusions. Moreover, as privacy intrusions increase and previously private information becomes public, the sphere of what remains private necessarily diminishes. The obverse of falling costs to privacy invasion therefore is that the cost of maintaining any given level of privacy is increasing—i.e., the marginal cost curve of privacy is shifting to the left.

As the value of privacy rises, owing to its increased scarcity, it becomes increasingly attractive for individuals to specify the conditions under which such privacy will be protected. For example, one might expect to see the emergence of ratings services that evaluate and publish the performances of plans and providers regarding how well they protect individual patient privacy. One might also expect to see the emergence of health plan offerings tailored to different privacy preferences.[12] We might also expect to see the emergence of legislation and regulations as individuals seek to describe and protect their rights in law. The important point of the foregoing is that as a right (in this case medical privacy) becomes more valuable, individuals will likely take steps among themselves (contractually), and collectively (through the political process) to specify and defend those rights.

We suggest that a clearer delineation of property ownership rights, including the control and disposition of information, would preclude the need for a complex rule with its attendant bureaucracy and costs. Given the variety of preferences for privacy—not to mention the different prices individuals face to maintain those preferences—it is difficult to imagine a set of blanket protections that could be fashioned that would still protect each individual's privacy (yet remain commensurate with their preferences and budgets). In our increasingly custom-tailored world—itself in no small part attributable to advances in technology—it is ironic that HHS has attempted to graft a one-size-fits-all mandate onto the medical privacy needs and rights of Americans. We therefore urge the Department to give more careful and thoughtful consideration to the implications of privacy and of property rights so that HHS and the federal government can strike the appropriate balance between access and privacy.

The protections HHS is attempting to set up take preliminary steps toward achieving the important end of protecting patient privacy (including records kept by the federal government). The rule for example puts those who collect and distribute patient information on notice that cavalier treatment of this confidential information is not acceptable. In spite of valiant attempts however, the proposed rule suffers from a number of crucial weaknesses that may end up bringing about precisely the consequences HHS is ostensibly trying to prevent.

[12] For example, individuals might be induced to make their private health information public in return for health insurance discounts, as the insurer resells the information to say, a pharmaceutical research firm.

III. Strengths and Weaknesses of the Proposed Rule

In this section, we focus on the strengths and weaknesses of the proposed rule (i.e., those most likely to generate unintended or adverse consequences). We begin with the fact that the rule eliminates current routine collection of patient authorizations at the point of service and instead places a complex rule in the place of individualized control. Second, the rule affords only limited protections against law enforcement officials' access to health records. Third, the rule paves the way for imposition of a national identity card for every citizen and an associated national database of individually identifiable health information. Fourth, the rule overrides state-level protections with a one-size-fits-all federal rule. Lastly, the rule does not address the ambiguity regarding property rights in the data once they are collected.

A. Removes Authorization for Payment, Treatment, and Operations

The proposed rule seeks to prohibit collection of medical release forms that are now routinely gathered at the point of service. Hospitals for example, may no longer obtain signed authorizations for treatment and the related release of information, since the proposed rule provides blanket exemptions for release of information related to payment, treatment, and other health care operations. The Department claims that the signatures obtained on current forms constitute neither informed nor voluntary consent and should therefore be eliminated.

In claiming that the existing authorizations are coercive, HHS suggests that patients are compelled to sign traditional releases or risk having treatment withheld. However, HHS offers no substantiation of this claim in the proposed rule. Treatment is not withheld even when a patient refuses to sign. To illustrate this fact, consider that unconscious individuals (or those who for some other reason cannot tender legal consent) routinely receive treatment in hospital emergency rooms.

Another critical aspect of the current regime, even given its claimed weaknesses, is the implicit protection afforded to physicians insofar as their Hippocratic Oath is concerned. On their oath, doctors have sworn to protect the confidentiality of a patient's medical records as well as the conversations patients have with them. This is not an arbitrarily chosen obligation. Without the patient's trust that disclosures will be treated confidentially, patients may not be entirely honest with their physicians, and therefore, incorrect or incomplete courses of treatment may be prescribed as a result. By signing the waiver, the patient releases the physician (at least implicitly) from his/her oath, and permits the doctor to provide information relevant for treatment and other purposes. Without the release, one can imagine that a rational course for a physician to follow might be to continue requiring patients' signatures on pro forma releases, and absent such signature, to refuse to release any information to any other person for any reason.[13]

[13] The proposed rule anticipates this eventuality by making even voluntarily signed releases for purposes of treatment, payment, or other health care operations illegal. "We also propose to prohibit covered entities from seeking individual authorization for uses and disclosures for treatment, payment, and health care operations unless required by State or other applicable law." Proposed Rule, p. 59941.

It is unclear what the advantages are of *not* obtaining routine releases in connection with payment, treatment, and health care operations, especially since such releases are already obtained today, and the procedures and policies are already well understood. HHS has not argued that paperwork burdens will be reduced significantly by the proposed change. Nor has it argued that current policy impedes the flow of medical services. HHS may be right that "such authorizations could not provide meaningful privacy protections or individual control and could in fact cultivate in individuals erroneous understandings of their rights and protections." However, as noted above, the proposed rule offers little to address this problem either and, in fact, it makes matters worse in some respects.

The proposed rule seeks as a general principle to protect and enhance doctor-patient confidentiality, but at the same time, it takes contradictory positions in this regard. As the proposed rules states, "Health information is considered relatively 'safe' today, not because it is secure, but because it is difficult to access. These standards improve access and establish strict privacy protections."[14] This statement seems to recognize that providing improved access to patient health care records without other safeguards would mean degraded privacy. However, whether the protections proposed by HHS are sufficient to protect privacy from this greater access is unclear, given the blanket provisions for information release under the rule.

B. Exceptions for Law Enforcement

The proposed blanket exception allowing law enforcement access to medical records may pose particular problems for protecting patient privacy. Under an urgency standard, an officer of the law need merely *represent* that disclosure of protected health information is necessary if "an individual … is or is suspected to be a victim of a crime, *abuse, or other harm*, if the law enforcement official represents that: (i) [protected health information] is needed to determine whether a violation of the law by a person other than the victim has occurred; and (ii) immediate law enforcement activity that depends upon obtaining such information may be necessary."[15] [Emphasis supplied.]

The idea of good faith disclosures by health care providers raises another major concern regarding law enforcement.

> Because the regulation applies to covered entities, and not to the law enforcement officials seeking the protected health information, the covered entity would not be in a position to determine with any certainty whether the underlying requirements for the process have been met. …In light of this difficulty facing covered entities, the proposed rule would include a good faith provision.[16]

[14] *Ibid*., p. 59928. This is the Court's "practical obscurity" protection surfacing again.

[15] *Ibid*., p. 60057.

[16] *Ibid*., p. 59963.

In other words, the good faith exclusion is an attempt to relieve health care providers from damages arising from the release of confidential health care information under misrepresented circumstances. That is, the good faith exclusion attempts to remedy one defect (the potential for unlawful access to medical records) with yet another qualification to the general rule protecting privacy.

Doubtless, there are circumstances where the urgent needs of law enforcement may take precedence over rights to privacy. The questions at issue however, are (a) whether such emergency circumstances are clearly proscribed so that the potential for official abuse and misjudgment are minimized, and (b) whether, in our zeal to capture lawbreakers we trample the rights of the law-abiding. The Constitutional protections afforded by the Fourth Amendment and elsewhere exist mainly to protect citizens from the state and its agents. Yet, it is the government that is given substantial discretion to peruse private medical records. To the extent enforcement officials require access to medical records, HHS has failed to show why due process, including an impartial review by a competent judicial authority to check for probable cause, should not be followed.

C. Exceptions for National Health Care Data Collection (§ 164.510 [g])

HHS proposes to permit disclosure of protected health information without an individual's authorization "when such disclosures are authorized by State or other law in support of policy, planning, regulatory, or management function."[17] These last four broadly drawn categories could encompass nearly any governmental function one might care to name.

No doubt, *generalized* data (or personally unidentifiable information) concerning rates of admission, treatment, discharges, and so on can be valuable to governmental officials in policy analysis. However, HHS does not offer justification for allowing detailed patient-level data collection by state and federal authorities, other than the observation:

> The data are an important resource that can be used for multiple policy evaluations. The collection of health care information by governmental health data systems often occurs without specification of the particular analyses that could be conducted with the information.[18]

While the data may be important for policy evaluations, the research importance must be more carefully weighed against the interests of individuals to keep their health care records private. In addition, symmetry would imply that records used in non-profit research be afforded the same level of protection as records used in for-profit research.

[17] *Ibid.*, p. 59964.

[18] *Ibid*., p. 59964

D. Paves the Way for a National Medical Records System and the Unique Health Identifier

To facilitate implementation of a national medical records database and its associated unique health identifier, strong privacy protections must first be in place. The proposed rule, by attempting to preserve privacy, helps to pave the way for the imposition of a national identity system and database. Unfortunately, it our belief that individual medical records may not be protected, and in any event will be easily accessible by government officials.

Inquisitive or meddlesome government officials may be inclined to search medical records of celebrities, neighbors, or even enemies. While the proposed rule carries penalties for such behavior, it is well to recall that there are penalties against IRS employees who inappropriately access or use private tax data. However, violations persist, perhaps indicating that for sanctions to be effective, they must be set higher than they are in the present rule.

A nationwide database of medical information would doubtless have many advantages. Infectious disease control, drug research and development, and cost control are but a few of the uses to which such an information set could be put. However, our concern is that without adequate privacy safeguards, the value of that database will diminish as the accuracy of its data diminishes.

E. Overrides State-level Protections

The proposed rule negates state-level protections of medical privacy. Every state currently affords some level of affirmative protection of patients' rights to privacy and protection for their medical records.[19] The protections vary from state to state and HHS argues that state-to-state inconsistencies make medical privacy uneven across the US. While this is true, the Department does not provide adequate analysis of the benefits from uniformity.

Among the benefits of a uniform federal approach is the fact that federal rules will provide a consistent, *de minimus* standard no matter where one obtains medical care in the US. Certainly, some states with stronger privacy protections may see diminishment in their standards, but importantly, states with weak protections will be advanced. In addition, plans and providers who operate across multiple jurisdictions should see lower costs from application of a single rule.

A federal standard does not necessarily offer uniformly better approach to protecting medical privacy. In fact, under the present system, if privacy were an overriding concern for a given patient, the patient today at least has the *opportunity* to seek out states and localities where privacy protections more closely comport with his/her preferences. Under a one-size-fits-all approach however, HHS forecloses even this limited opportunity, leaving no other option except to conform to the federal government's idea of what is best in the area of privacy.

[19] See Tomes, Jonathan, *Healthcare Privacy and Confidentiality: The Complete Legal Guide,* (Chicago: Probus Publishing, 1994), pp. 1-6 and *passim*.

Uniformity also forecloses the opportunity to innovate at the margins with respect to privacy. It is important to recognize that there are also patients to whom medical privacy is unimportant, but who will be bearing the cost of privacy protections that they do not value. In addition, for those consumers to whom medical privacy is of paramount concern, it is entirely possible that the minimum standards proposed by HHS may, in effect, become maximum standards.

F. Does Not Adequately Address Property Rights in Information

One of the chief difficulties associated with protecting health care privacy stems from ambiguity over who owns the property rights to individual health care information, once it is collected.[20] If the property rights belong to the patient, any misuse or misappropriation of the information would constitute an actionable offense to the aggrieved individual. Conversely, if the plans and providers who collect it owned the information, then a different set of outcomes and recourse emerge. Unfortunately, HHS does not address this central issue.

Rather than developing an entire complex of new rules and official enforcers to protect the privacy of patients' medical records, HHS would do better to examine whether property rights over those records have been adequately defined. Based on such an analysis, it could then design policy that aligns with those property rights such that medical privacy is optimally protected. In the following section, we suggest one means of coming to grips with the issue of who owns medical information and consider the likely consequences of different ownership patterns.

IV. Ownership of Medical Information

Who *owns* individually identifiable medical information? HHS never asks this question in the 150 pages of its proposed rule. The answer to the question however is crucial because depending in whom such rights are vested determines both the level of privacy that can reasonably be expected, as well as the care that individuals can be expected to demand given a certain level of privacy protection. In this section, we sketch one approach to evaluating different property rights (i.e., ownership) patterns in medical information.

In our estimation, there are essentially three distinct patterns of ownership of individually identifiable medical information: (a) individual patient ownership (i.e., the subjects or generators of the information); (b) plan or provider ownership (i.e., the collectors of the information); and (c) government ownership. Table 1 below suggests one possible framework for analyzing these three main ownership assignments in medical information. The dimensions we consider include

[20] As stated above, in many states, the plans and providers who collect medical information are the actual owners of this information. The proposed rule could have benefited from making ownership by someone—either plans and providers or the individual patients—explicit.

- Transactions costs (i.e., the costs of executing and enforcing contracts associated with a particular rights assignment);
- Rule specificity (i.e., whether detailed rules are required to protect the information owner);
- The number of checks and balances available to protect against promiscuous disclosures;
- Whether or not an assignment automatically aligns incentives to protect with preferences for protection; and
- The likely consequences of a particular assignment on the health of the population.

TABLE 1
SUMMARY OF ALTERNATIVE OWNERSHIP PATTERNS IN MEDICAL INFORMATION

Owner	Transactions Costs	Rule Specificity	Number of Checks?	Built-in Incentives to Protect?	Health Care Consequence
Individual	Medium	General	(3) Individual, Market, Government	Yes	Status Quo or Slight Degradation
Plan/Provider	Low	General	(3) Individual, Market, Government	Yes	Status Quo
Government	High	Detailed	(1) Government	No	Degradation

A. Individual Ownership

One could imagine the simplest case of individual ownership of medical information as the case where an individual takes physical possession of those records previously in the possession of her doctor and/or insurance plan.[21] In the simplest case, every time an individual sought medical care, the individual would need to bring his/her records when he/she encountered the health care system. The potential for loss and incomplete information makes this arrangement—given the present state of technology—a more costly alternative than the current state of affairs.[22] Thus, transactions costs may tend to be higher than if

[21] An alternative arrangement of course consists of establishing a bailment or fiduciary relationship wherein the individual owns the information but the health care plans and providers continue to collect and maintain acting as an agent on behalf of the individual.

[22] The current state of affairs with respect to ownership of individually identifiable health information is closest to the plan/provider arrangement; wherein the collector of the information is the de facto owner of that information even though that information is of a deeply personal nature about someone else.

ownership were assigned to plan and providers. (This may not be the case however if a fiduciary arrangement were established.)

An advantage of the individual ownership arrangement is that detailed rules and regulations governing privacy protection are not required since existing rules of property, contract, and tort can be called into service by the individual as well as by health care plans and providers to work out mutually satisfactory agreements. Also, since individuals (including regulators) are not omniscient, a non-regulatory approach offers the advantage of flexibility. That is, a rule typically must be designed to foresee as many permutations and interpretations as possible if it is to achieve the outcomes sought by the legislators and their regulatory agents. Such a process necessarily begets complex rule, but a complex rule begs the question of who is in a better position to determine one's privacy requirements: a regulator or the individual himself?

An individual can implicitly rely on himself to protect his own property to the degree he wishes. Importantly, the individual can also rely on market forces of competition for profit (and the prospect of potential losses) to ensure that he receives the degree of privacy protection commensurate with his preferences and willingness to pay. In addition, the government, in its judicial capacity, operates as a backstop in this arrangement to adjudicate among individuals, plans, and providers when disputes over information ownership emerge. Thus, three different checks operate independently to ensure that an individual receives the level of privacy he or she wishes. With the exception of adjudication, the incentives to protect privacy operate more or less automatically.

Since individual ownership entails transactions costs beyond the status quo however, a likely consequence may be a slight degradation in health care to the individual as resources are diverted to ensuring privacy protection rather than to the provision of health care. This degradation should be slight, and in any case will likely be offset by those reentering the health care system who value privacy highly once it is seen that the system affords clear and defensible ownership in individually identifiable health information.

B. Plan/Provider Information Ownership

As we stated above, plan/provider ownership of individually identifiable health information is the current *de facto* arrangement—although it is not clearly recognized as such by HHS. Inasmuch as plans and providers go the expense of collecting and maintaining patient level information, plans and providers are customarily treated as the owners of the information—subject to limitations they may agree to with the individual subjects of the information. Explicit legislative recognition of the existing pattern, therefore, would entail little in the way of incremental transactions costs compared to the current mode of operation.

As in the case of individual ownership, plan/provider ownership obviates detailed rules and regulations since the preexisting rules of property, contract, and tort can be employed. In addition, the number of checks and balances would be the same, and would be operating in both the individual's as well as the plan's favor. That is, not only could individuals seek the plans offering the privacy protections commensurate with their preferences for privacy, but

also plans and providers could tailor their offerings to appeal to those patients whose privacy requirements comport with the plan's.[23] Privacy ratings agencies will emerge (as they already have on the Internet) to evaluate the privacy protection afforded by different plans and providers.

The consequences of plan/provider ownership in terms of societal health would be similar to the current state of affairs, but with the likely addition of those currently avoiding health care because of privacy concerns. In other words, once it becomes known that privacy protection is an important business consideration (i.e., that violating privacy has cost consequences for businesses) one can expect plans and providers to tailor their privacy offering more closely with those desired by their customers.

C. Government Health Information Ownership

The underlying theme and tone of the proposed rule seems to suggest that HHS is attempting to establish *de facto* government ownership of private medical information, with little regard for the potential consequences. However, this is unlikely to result in a superior outcome to the preceding arrangements, nor will it comport with the ostensibly desired outcome stated in the supporting documentation for the proposed rule of improving privacy and therefore access to medical services.

The proposed HHS rule entails an incremental establishment and compliance cost that plans and providers must incur in order to obey the law. These costs are discussed in the Costs and Benefits section below; however, for purposes here, we estimate additional incremental costs approximately nearly one billion dollars per year. Our analysis indicates that the transactions costs of engaging the US health care system will be higher under a centralized rule than without one.

In addition, since the rule cannot possibly anticipate every avenue of "innovation" within the letter of the law, we can reasonably expect individuals, plans, and providers to find ways at the margin to circumvent the rule if it impedes delivery of health care. For example, physicians may become less inclined to note detailed patient conditions if they view such notations as possible avenues for privacy invasion. Patients might actually take additional steps (even more than they do presently) to avoid the traditional health care system if they realize their health care information might be collected in a centralized government database. In other words, the rule may generate precisely the opposite effect of that which is ostensibly intended.

It is important to note that if government were to assume ownership and control of this information (as HIPAA requires through implementation of a nationwide medical records database), individuals who are the subject of this information will have little recourse in the event of a violation. Sovereign immunity will preclude attempts to seek civil redress for aggrieved individuals. Indeed, the only check on promiscuous disclosure of private health

[23] One could imagine a scenario for instance, where a health insurance plan might offer a discount if the individual participant were willing to release his/her information for purposes of pharmaceutical research, say.

care information will be the government itself. That is, the safety of the information will depend vitally on the goodwill and conscientiousness of government officials who design the database as well as those who administer it. Market and individual checks on promiscuous disclosure will be conspicuous by their absence.

If health care data were eventually centralized in a government owned and controlled database, the chances for improper disclosure increase radically (as HHS implicitly seems to understand). Even if the chances for improper disclosure are identical to those where records remain privately owned and maintained, the potential for damage is necessarily greater when government owns and controls the data inasmuch as an entire nation's worth of data can potentially be disclosed at once rather than the limited (albeit still damaging) disclosure that is possible under present circumstances. The important fact to bear in mind with respect to privacy invasions is that once data are released into the public domain, the damage is done. That is, once the bell rings, it cannot be unrung, and the crucial point is that the bell has the potential to ring much louder under government control than under private control.

This digression on ownership and property rights suggests that a complex regulation may not be the best or even only solution to a knotty problem like privacy. The first premise when considering potentially intrusive and complex regulations might well be an explicit recognition that individual adults are at least as competent as regulators to determine their own needs for privacy and are in fact quite capable of effectively lodging those demands with providers.

V. Costs & Benefits of the Proposed Rule

In spite of the detailed work on costs and benefits contained in the proposed rule, the estimates and estimating procedures fall short of the mark of providing an accurate assessment of the rule's potential costs and benefits. Perhaps an indication of the difficulties and contradictory findings HHS encountered was apparent to the rule's drafters early on. On page 59922 of the proposed rule for example, HHS states in part, "Thus, even if the rules proposed below were to impose net costs, which we believe they do not do, they would still be 'consistent with' the objective of reducing administrative costs for the health care system as a whole." It is unclear what HHS means by this contradictory statement.

Our own analysis of costs and benefits suggests that, on balance, the rule in its currently proposed form may in fact increase health care costs. Moreover, in light of the limited protections afforded by the rule, and of the unsubstantiated benefits the rule's authors suggest will accrue from its imposition, the proposed protections, while desirable in principle, do not in fact confer net benefits. The proposed rule may lead to diversion of resources away from actual health care services, and in the final analysis, the rule may lead to less privacy not more and therefore to poorer overall health for Americans.

In the following sections, we summarize our cost estimate findings. More extensive documentation of our estimates appears in Appendix II. Following the lead of HHS, we have divided our cost estimates into those which may be classified as (a) one time or start up costs

and (b) ongoing costs. Start up costs are of course those costs incurred in order for health care plans and providers to initiate compliance with the proposed regulations initially. Ongoing costs are those costs that recur with some frequency by virtue of the imposition of the proposed regulation.

It is important to note that HHS does not furnish cost estimates for a number of requirements that will be imposed by the new rule.

> The areas for which explicit cost estimates have not been made are: The principle of minimum necessary disclosure; the requirement that entities monitor business partners with whom they share PHI [private health information]; 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 regulations. [24]

One potentially important cost that HHS does not consider in its analysis is the regulation's requirement that covered entities monitor compliance among their business partners.[25] We include estimates of the cost of this aspect of the proposed rule in the one-time cost section below.

In developing our estimates below, we rely on the HHS assumption that there are 18,225 health care plans in the US, and 871,294 US health care providers who would fall under the proposed rule.[26] "Health care plans" include insurance companies, HMOs, or group plans that provide or pay the cost of medical care.[27] A "health care provider" on the other hand, is one "who furnishes, bills, or is paid for health care services or supplies in the normal course of business."[28]

A. One-time or Start Up Costs

We consider the following one time or start up costs of bringing a plan or provider into compliance. These parallel the cost categories for which HHS provides estimates with the exception of item 6, business partner contract review.[29]

> (1) Analysis of the significance of the federal regulations on covered entity operations;

[24] Proposed Rule, p. 60015.

[25] §164.506 (e) (1) (ii) of the proposed rule states that "a covered entity must take reasonable steps to ensure that each business partner complies with the requirements of this subpart with respect to any task or other activity it performs on behalf of the entity, to the extent that the covered entity would be required to comply with such requirements." *Ibid*., p. 60054.

[26] The number of plans and providers appears in Table 1 of the Proposed Rule, p. 60007.

[27] *Ibid*., p. 60050. §160.103, "Definitions."

[28] *loc. cit*.

[29] *Ibid*., p. 60015 and *passim*.

(2) Development and documentation of policies and procedures;

(3) Dissemination of such policies and procedures both inside and outside the organization;

(4) Changing existing records management systems or developing new systems;

(5) Training personnel on new policies and systems changes; and

(6) Business partner contract review.

Table 1 below summarizes both the HHS start up cost estimates as well as those developed by the Mercatus Center's Regulatory Studies Program (RSP). (To reiterate, our previous submission contains the details of our estimating procedure.)

TABLE 1
SUMMARY OF ONE-TIME COSTS OF THE PROPOSED REGULATIONS ON MEDICAL PRIVACY
($ Millions)

Cost Category	HHS Estimates	RSP Estimates
Initial Legal Analysis of Applicability	$ 395.0	$ 686.0
Policy Development & Documentation		609.9
Policy Dissemination	105.9	67.9
Update Electronic Records Management Systems	90.0	393.3
Initial Training in Privacy Policies	22.0	116.9
Business Partner Contracting	N/E	89.0
TOTAL One-Time Cost Estimates	**$ 612.9**	**$ 1,963.0**

HHS estimates these costs at $613 million. Our estimates by comparison place this burden at **$1,963 million**. The major differences in the estimated results owe to a more careful consideration of the actual opportunity costs (both in terms of time and money) involved in start up compliance, as well as from our explicit consideration of business partner oversight. HHS estimates a weighted average start up cost per provider cost of $375 and an average per plan cost of $3,050. Our estimates by contrast place this average burden at $1,960 and $16,100 respectively.

B. Ongoing Costs of Compliance

A partial list of the ongoing costs of implementing the proposed rule include:

(1) Patient requests for access and copying of their own records;

(2) Patient Requests to Amend or Correct Records;

(3) The need for covered entities to obtain patient authorization for uses of protected information that had not previously required an authorization;

(4) Dissemination and implementation both internally and externally of changes in privacy policies and system changes;

(5) Periodic re-training of personnel on policies; and

(6) Periodic review and oversight of business partners.

Table 2 below summarizes both the HHS ongoing cost estimates as well as those estimates developed by the Mercatus Center's Regulatory Studies Program (RSP).

TABLE 2
SUMMARY OF ONGOING COSTS OF THE PROPOSED REGULATIONS ON MEDICAL PRIVACY
($ Millions)

Cost Category	HHS Estimates	RSP Estimates
Records Inspections and Copying	$ 81.0	$ 49.4
Amendment and Correction Requests	407.0	405.0
Patient Authorizations	54.0	477.0
Periodic Policy Disseminations	83.4	17.0
Periodic Re-Training of Personnel	22.0	39.0
Periodic Business Partner Compliance Review	N/E	0.0
TOTAL Ongoing Cost Estimates	**$ 674.4**	**$ 987.4**

The major areas of estimate disagreement hinge on "Patient Authorizations," and "Business Partner Oversight." In the former category, we accepted the HHS assertion that roughly one in six people are currently taking some steps (including treatment avoidance) to preserve their privacy. Therefore, this ratio seems a logical starting place to estimate the number of persons who might actively try to prevent disclosure of their health information through authorizations.

C. Some Comments on Business Partner Compliance Oversight (§164.506 [e])

HHS did not furnish estimates for the ongoing costs of monitoring business partner compliance with respect to protected health information. However, the proposed rule requires that, "a covered entity would be responsible for assuring the each such implementation standard [for ensuring privacy of protected health information] is met by the business partner. … We are proposing that covered entities be accountable for the uses and disclosures of protected health information by their business partners. A covered entity would be in violation of this rule if [it] knew or reasonably should have known of a material

breach of the contract by a business partner and it failed to take reasonable steps to cure the breach or terminate the contract."[30]

This aspect of the proposed rule shifts the burden of law enforcement from HHS to the plans and providers. To evaluate a range of costs of this burden shift, assume that in order to prevent potential liability, at a minimum, covered entities request letters from business partners certifying the partners' compliance with the contract terms regarding privacy. Such an approach could be relatively inexpensive for the covered entity. However, since a letter may prove insufficient to insulate a plan or provider from proving "it did not know or could not have known" that a breach had taken place among its partners, this approach also poses potential liability risks, with associated costs (which we have not attempted to estimate).

D. HHS Benefit Estimates Overstated

HHS estimates on the benefits of the proposed regulation rely heavily on anecdote and unsubstantiated inferences. At bottom, the estimates rely on postulated, but largely unsubstantiated causal linkages between increased privacy and earlier diagnosis and medical treatment.

To be sure, early disease detection and treatment offer significant health benefits, and this is clearest in the cases of cancer and HIV that HHS uses to illustrate its point. However, it is an improper inference to suggest that loss of doctor patient confidentiality is the critical component leading to delayed treatment without any supporting evidence to support such a claim.[31] In the cases of breast and ovarian cancers for example that HHS cites, "early detection of these cancers could have a significant impact on reducing loss due to disability and death."[32] This is no doubt true, but one cannot logically make the jump to the inference that impaired privacy is the principal cause of delayed testing and treatment.

Loss of privacy clearly plays some part in delayed treatment, but the crucial question is how much? With respect to mental health, HHS makes a more controlled attempt to estimate the benefits owing to the relationship between increased privacy and increased early treatment. "Given the existing data on the annual economic costs of mental illness and the rate of treatment effectiveness for these disorders, coupled with assumptions regarding the percentage of individuals who might seek mental health treatment under conditions of greater

[30] *Ibid*., p. 59949.

[31] In the proposed rule (p. 60020), HHS states, "Thus, despite the potential benefits that early identification of cancer may yield, many researchers find that patient concerns regarding the confidentiality of cancer screening may prevent them from requesting the test, and result in disability or loss of life." This vague statement immediately begs the questions: how "many researchers find that," and to what degree is early detection attributable to loss of confidence versus other, confounding factors? HHS does not indicate answers to these important qualifying questions.

[32] *Ibid*., p. 60020.

privacy protections, the potential additional economic benefit in this one treatment area could range from approximately $208 million to $1.67 billion annually."[33]

An important consideration when viewing the benefits of the proposed regulation is that the numerous exceptions we examined above in connection with the rule's weaknesses will operate to negate any potential benefits by actually undermining citizen confidence that the proposed rule will increase privacy. If patients know for example that their medical records may enter a national database that is accessible by government agents and others for listed purposes, the tendency may be to avoid contact with the health care system if privacy is a significant concern.

E. Net Costs and Benefits

HHS has provided only one area where increased privacy may result in significant benefit, mental health. Therefore, in order to balance costs and benefits, let us consider the ongoing costs that we calculated earlier (plus the initial up-front costs of compliance) as the basis against which any supposed benefits must exceed in order to justify imposition of the rule.

Using the OMB standard seven percent discount rate, and assuming that ongoing costs will recur year in and year out, the discounted present value of the ongoing costs is approximately $9.25 billion based on HHS estimates, and $14.1 billion based on RSP estimates. Add to these figures the one-time start up costs above, and a present value of all costs obtains totaling $9.86 billion using HHS estimates, and $16.1 billion using the RSP estimates.

To put these costs into some perspective, in 1996, a kidney transplant was one of the five most expensive hospital procedures, at $66,000 (excluding follow up procedures).[34] Let us assume that follow up care and rehabilitation drive the average cost of a kidney transplant to $200,000. If the entire burden of privacy costs were to fall on these procedures, it would imply that more than 80,500 kidney transplant operations would be foregone over the next several decades, as money is redirected instead toward implementing privacy protections. Given that in 1996 there were 12,080 kidney transplants performed in the United States, the cost of the privacy rules equate to more than six and a half years worth of kidney transplants potentially foregone if the burden fell on them alone.

The burden however, does not fall on one aspect of health care alone, but rather diffuses throughout the economy. Therefore, looking at the costs somewhat differently, our estimates suggest that the average American household will incur additional annual health-related

[33] *Ibid*., p. 60021.

[34] Source: *Hospital Inpatient Statistics* (1996), Agency for Health Care Policy Research, AHCPR Publication No. 99-0034.

expenses of roughly $160 over the next several years in order to safeguard their medical records.[35]

While such costs, when viewed in isolation, may not seem extraordinary, when balanced against the vague benefits the rule confers, the costs seem quite high indeed. In fact, when the costs are then balanced against the potential erosions that the rule may bring in its train (i.e., through the establishment of national records database, the unique health identifier, and the removal of authorizations for payment, treatment, and health operations, and so on), and the fact the above estimates omitted the costs of several features of the proposed rule, the costs grow larger still.

One last means of assessing regulatory costs in human terms is offered in a study by Lutter, Morrall, and Viscusi, which indicated that for every $15 million of increased regulatory costs, on average, one statistical life is lost.[36] The HHS estimate of costs suggests that (statistically) perhaps 650 persons may lose their lives because of the imposition of these rules. The RSP estimates on the other hand, suggest statistically that about 1,075 persons may lose their lives over the course of the proposed rule's existence.

VI. Conclusion: Less Privacy, Higher Costs, and Lives Lost

We estimate that the proposed rule may cost nearly a billion dollars a year for the aspects of the rule we can reliably estimate, plus another two billion dollars in up front costs. If the rule conferred tangible privacy benefits, as its preamble suggests, these costs might be worth incurring. However, the rule in its currently proposed form offers limited tangible privacy benefits, and in fact erodes current protections, while it significantly raises health care costs in the US at the same time.

Given the limited benefits and high costs, in its currently proposed form this rule may ultimately damage the long-term health of Americans. Indeed, it is altogether likely that the rule may generate perverse results such as *less* privacy—owing to the pervasive availability of information and increased access by government agencies to the private medical records of individuals. A less healthy citizenry may be the consequence as individuals reduce prevention and treatment visits owing to increased costs and decreased privacy.

Inasmuch as the most important rule of sound medical care is to first do no harm, we urge the Department of Health and Human Services to modify these rules with an eye toward reducing their cost impact, and constraining law enforcement access to private health information without following due process. We also urge the Department to examine whether property rights over private medical records are clearly and adequately defined.

---

[35] The number of US households is a 1997 estimate (101,018,000) taken from the *Statistical Abstract of the United States* (1998) and is based on Table No. 69, "Households, Families, Subfamilies, and Married Couples: 1970 to 1997." US Census Bureau, "Current Population Survey."

[36] Lutter, Morrall, and Viscusi (1999), "The Cost per Life Saved Cutoff for Safety-Enhancing Regulations," *Economic Inquiry 37* (4), pp. 599-608.

Appendix I
RSP Checklist
HHS Health Care Privacy Regulations

Element	Agency Approach	RSP Comment
1. Has the Agency identified a significant market failure?	HHS proposes a national rule to protect private health information. **Satisfactory**	Property rights in health information are ambiguously defined and defended. While HHS implicitly recognizes this, it would do better to examine the root cause of this problem, and address the definition of property rights directly.
2. Has the Agency identified an appropriate federal role?	HHS simply asserts a federal role without substantiation or consideration of state-level achievements **Unsatisfactory**	HHS is seeking to impose a regimented national rule that ignores local circumstances. The proposal includes a number of blanket exceptions and qualifications to address different circumstances, when a more targeted or tailored approach, consistent with federalism principles, would be more appropriate.
3. Has the agency examined alternative approaches?	HHS has considered alternatives within the rubric of a federally imposed rule. **Fair**	HHS excluded non-federal alternatives from active consideration. It also failed to consider market-based approaches and the establishment of clearer property rights to private medical information.

4. Does the Agency attempt to maximize net benefits?	Within the confines of the cost benefit HHS makes, it does attempt to balance them. **Fair**	HHS cost estimates contain omissions and inconsistencies. Benefits mostly remain unquantified. The agency does however net the two against each other.
5. Does the proposal have a strong scientific or technical basis?	HHS does not providing substantiation and documentation for its rule justification and cost estimates. **Unsatisfactory**	HHS relies on undocumented polls to justify imposition of the rule. Also, plausible alternative assumptions significantly increase the estimated costs of the proposed rule.
6. Are distributional effects clearly understood?	The preamble does not address the unintended consequences likely to emerge. **Unsatisfactory**	The blanket permission for law enforcement access to private records in particular could have disproportionate effects on some individuals' willingness to undergo medical treatment. Furthermore, to the extent the rule increases health care costs, low income and uninsured individuals would be most harmed.
7. Are individual choices and property impacts clearly understood?	The proposal does not focus on the key issue of property rights to private medical information, nor does it recognize the effect different regulatory approaches would have on individual choices. **Unsatisfactory**	HHS should examine whether property rights over private medical records are adequately defined. Based on such an analysis, it could design a policy that aligned those property rights such that medical privacy is optimally protected. It should also consider unintended actions the rule could facilitate, by law enforcement agencies for example.

Appendix II
Estimating Techniques and Data Sources
Proposed HHS Health Information Privacy Rule

I. Compliance Start-Up Costs

A. Analysis of Applicability (§164.522 and passim)

Here we are concerned with an initial analysis of the regulation's applicability to a particular health care enterprise. Few covered entities are likely to introduce new policies and programs—even those offered by their respective professional associations—without first seeking competent legal advice. As the privacy rules constitute a new area of regulation, and the risks from non-compliance are high (as indicated by the high sanctions per violation[37]), legal oversight of applicability is simply prudent.

Currently, 62 percent of the 871,294 providers would seek legal advice as to how best comply with the rules. This percentage corresponds to the number of providers who currently maintain medical records electronically.[38] Assume legal advice to providers takes eight hours on average, at a national average cost of $125.00 per hour for outside legal counsel, or $1,000 per establishment. Of the 18,225 health care plans that fall under this regulation, assume all of them use electronic record keeping and are therefore covered by the rule. Plans would obtain legal advice from in-house legal staff at an average opportunity cost of $100.00 per hour. HHS estimates that plans might be expected to spend roughly ten times more than providers reviewing the regulations owing to the larger scope of their operations as well as the myriad differing state laws to which many are subject.[39]

Based on the above considerations, the cost of determining the initial applicability of the proposed privacy regulations for both plans and providers is estimated at **$686.0 million**. HHS does not make a separate cost determination for this aspect of start up costs, but rather includes it in their estimate of policy development and documentation costs, which we consider next.

B. Policy Development and Documentation (§164.520)

HHS suggests that national and/or state professional associations may assume the burden of providing standardized policies and procedures with respect to privacy protection. It is certainly possible that such associations may provide policy "boilerplate" policies, however, it does not necessarily follow from this observation that the exercise will therefore be cost-

[37] Unlawful disclosure of protected health information for purposes of commercial gain for example, under the proposed rule, may be subject to a fine of $250,000 and 10 years in prison. *Ibid*., p. 59921.

[38] *Ibid*., 60005-60006.

[39] See p. 60015 for additional justification of the ten times relationship.

free, or that covered entities will not incur costs separate from those of the professional associations to customize policies and compliance documentation.

Health care providers may spend an average of one business day (8 hours) developing privacy policies, and health care plans may spend an average of two business weeks (80 hours) owing to the larger scope and complexity of their operations.

To develop a unit cost estimate, we considered two different cases. In Case I, assume that an entity principal (e.g., a doctor in a private practice, or an executive of a health care plan) takes responsibility for developing and documenting privacy policies. For health care providers therefore, we estimated an hourly opportunity cost of a physician's time at roughly $129/hour.[40] This hourly rate yields a total cost estimate of $898.0 million for health care providers. For health plan executives, we assumed an hourly opportunity cost rate of $75.00,[41] which yields a cost estimate of $109.0 million for plans. Under Case I assumptions, development and documentation totals $1,007.6 million.

In Case II, assume that an "average" entity employee undertakes the development and documentation of privacy policies. In the case of health care providers, this reduces the average hourly opportunity cost to $26.41, and gives a total cost for providers of $184.0 million. For health care plans the average employee opportunity cost drops to $19.32, giving a total cost for plans of $28.0 million. The total cost of developing and documenting health care privacy plans, under Case II assumptions, is $198.0 million. While it may be unrealistic to assume that an "average" employee would undertake this difficult and risky responsibility, the Case II estimate nevertheless provides a lower bound to the development and documentation aspect of the proposed rule.

It seems likely that a mixture of principals and employees may work to develop and document privacy policies. We therefore report here and in the summary tables, a mid-point estimate of **$609.9 million** to develop and document privacy policies. Taken together, the analysis of applicability and the development and documentation of policies and procedures give a combined cost estimate of $1,295.9 million. These figures compare with HHS estimates for the both categories of just $395.0 million for both categories.

C. Policy Dissemination (§164.512)

To raise patient awareness of their rights to privacy, the proposed rules require that notice must be furnished at the next patient visit in the case of a health care provider, or through an initial mailing in the case of health care plans. Subsequent notifications will continue to be in person in the case of providers, and, in the case of plans, will be an additional component of other plan correspondence such as bills, or renewal notices. (The cost estimates of

[40] This figure is derived by dividing total Offices of Doctors of Medicine Revenues (SIC Code 8010) by 724,000 practicing physicians and assuming a 2,000 hour standard work year.

[41] This assumes a fully loaded labor cost for the executive of $150,000/year.

disseminating privacy policies internally—to plan and provider employees—falls under our training cost estimates.)

Assume that the cost of printing, stocking, and handling the privacy rights notices is $0.029 each. If the these notices must be mailed, then additional costs of envelopes, labels, labor associated with inserting, stamping, and so on, as well as first class (bulk rate) postage are incurred too. The extra mailing costs add another $0.295 to each notice. Assuming 397 million health care encounters per year,[42] health care providers may be expected to incur costs of $11.5 million in connection with initially notifying patients of their rights under the proposed rule. Furthermore, the fact that there are 174,100,000 Americans covered by private insurance plans[43] suggests that costs of notification for health care plans will initially be $56.4 million.

Our start up estimates compare to HHS estimates of $59.7 million for providers in year one, and $46.2 million for plans in the same period. Interestingly, providers must furnish notification with each service rendered, even though multiple providers may see a given individual in a given year. Some individuals therefore may receive multiple notices of their privacy rights in a single year resulting in duplication, waste, and potentially reducing the effectiveness of the message.

After the initial notification in year one, assuming similar patterns of insurance and system encounters—and assuming 3% annual growth in each category—yields an ongoing cost estimate of notification of $17.0 million in year two. Under the conservative estimates above, our five-year estimate of policy dissemination therefore is $139.0 million. This compares to an HHS estimate of $231.0 million over the same five-year period.[44]

D. Changing Records Management Systems (§164.515 and 164.518[c])

We conducted a "bottom up" estimate of the requirements to modify existing computer systems required to accommodate the changes proposed in the privacy rules. First, we estimated the cost of including encryption software to ensure security of data during transmission to business partners and others. Such security may already be required for other HIPAA-related requirements, and so our inclusion of it here may constitute double counting. However, in the interests of completeness (and because it represents only 3% of our computer cost estimate) we include it here. Therefore, assuming again that 62% of providers require computer upgrades, and that the encryption software average $50.00 per plan and provider installed, the total estimated cost of encryption security software is $27.9 million.

---

[42] "Data from the 1996 Medical Expenditure Panel Survey show that there are approximately 200 million ambulatory care encounters per year, nearly 20 million persons with a hospital episode, 7 million with home-health episodes, and over 170 million with prescription drug use …" *Ibid*., p. 60016.

[43] *loc. cit*. Estimate based on a 1998 National Health Interview Survey.

[44] HHS appears to be including internal policy dissemination costs in its policy dissemination cost estimates. We have chosen instead to include these in our estimates of training expenses.

Next, are the costs associated with modifying patient-related computer software modules. Included in this category are such subsystems as billing, accounts receivable, and patient records. Assume that all three subsystems could be updated in 3 hours. In other words, programming audit trails, and updating locks would take just one business day.[45] In that time, not only would programming be completed but initial evaluations and requirements assessments would also be completed. In addition to the three hours for the programming of audit trails and locks, one hour was included to program and install notices and disclaimers warning potential intruders that data are protected and illegally accessing it constitutes a crime.

To calculate the costs of this programming effort, take total revenues of computer programming services in 1996 (SIC Code 7371), and divide it by the total employment in that sector to arrive at a plausible estimate of the average hourly charge for programming services, which health care plans and providers might expect to incur. The estimated hourly rate is $59.49. The hourly rate times the estimated number of hours to upgrade the "front end" systems, yields an estimated cost of $132.9 million.

In addition, systems that deal with health care vendors and business partners must also be adjusted. Subsystems that control vendor accounts and accounts payable must be modified for the same reasons as patient accounts; that is, to incorporate audit trails, update locks, and to install notices and disclaimers. Assuming a similar amount of time is involved in modifying these "back end" support systems, and that unit costs are the same, the estimated cost is also $132.9 million

Lastly, both ends of the system will require testing and evaluation before going on line permanently to avoid data corruption and unexpected downtime. In addition, the electronic data interchange (EDI) interface will likely require modification and testing to ensure that communication with external business partners is functioning properly. Assume these testing and evaluation procedures add another three hours (2 hours to test the subsystems, and 1 hour to test the EDI interface) to the process, at a cost of $99.7 million.

Taken together therefore, we estimate the costs to modify the computer systems of providers and plans at **$393.3 million**. This compares to the estimate prepared by HHS of $90.0 million. HHS derives its estimate by assuming "if privacy constitutes 15 percent [of the security standard in HIPAA], then the security standard would represent about $900 million system cost. If the marginal cost of the privacy elements is another 10 percent, then the additional cost would be $90 million."[46] There may be simply too many unsubstantiated "ifs" to make the HHS estimate reliable.

[45] Audit trails are required in order to enable providers and plans to report to whom protected health information was released. Updating locks are required so that only authorized personnel could change records or adjust audit trails.

[46] Proposed Rule, pp. 60015-60016.

E. Personnel Training (§164.518[b])

HHS suggests that training costs will be minimal inasmuch as training of health care professionals is an ongoing process. "The ongoing costs associated with paperwork and training are likely to be minimal. Because training happens as a regular business practice, and employee certification connected to this training is the norm, we estimate that the marginal cost of paperwork and training is likely to be small. We assume a cost of $20 per provider office, and approximately $60-100 for health plans and hospitals."[47]

While training in general may be an on-going process, it does not follow that training in the protection of health care information will be an insignificant addition to the cost burden. We suggest that each employee who handles private health information will require training in order to (a) document to HHS that employees properly understand the importance of safeguarding it, and (b) to protect the firm from possible negligence insofar as unlawful releases of private health information are concerned. Also, rather than estimate training costs on the basis of plans and providers, we estimate the training burden based on the number of employees in the US health care system that may require training. By multiplying the number of hours spent in training by the average hourly wage, we obtain an approximate opportunity cost of training in terms of employment services foregone.

Three principal categories of health care employees will require training in the intricacies of privacy, including health services employees (doctors, nurses, hospital records clerks, etc.), health insurance employees, and pharmacy employees.[48] In total, these three categories of businesses employ 11,138,488, 623,389, 329,709 persons respectively. In each case, presumably only those employees who actually handle protected health information will require training. Therefore, we estimated that one-half of health services and health insurance plan employees will require training, while just 15% of pharmacy employees will require it.

Average wage rates of each employee class in turn were determined by taking total payrolls by SIC Code and dividing by the SIC employment, and assuming a standard 2,000 work year. The hourly wages costs averaged $15.05, $18.22, and $9.59 for health services, insurance, and pharmacies respectively. We assumed, conservatively, that employee training could be completed in one hour. Thus, the opportunity costs of labor foregone while in training totaled $87.7 million.

On top of the opportunity costs of labor services foregone by having individual employees attend training, we must add the cost of training materials and the trainer's time, as well as the certification that each employee must sign at the conclusion of training, as prescribed in the proposed rule. We estimated materials, trainer, and certification costs at an average of $5.00 per trainee, or an additional $29.1 million. Therefore, taking employee costs and

[47] *Ibid*., p. 60017. No evidence or inferences are given to support these cost estimates.

[48] The SIC Codes are 8000, 6320 + 6370, and 5190 respectively.

materials costs together gives a total training cost estimate of **$116.9 million**. This compares to an HHS estimate of just $22.0 million.

F. Business Partner Contract Review (§164.506 [e])

HHS is proposing that business partners with whom health care providers and plans share information be subject to contractual requirements for safeguarding protected health information. "The contract requirement we are proposing would permit covered entities to exercise control over the business partners' activities and provides documentation of the relationship between the parties, particularly the scope of the uses and disclosures of protected health information that business partners could make."[49] HHS elected not to estimate this cost as part of its cost/benefit analysis.

Because we think this aspect of the rule may represent a significant cost component, and because it represents a shift in the burden of law enforcement, we attempt an estimate. Three of five providers (or 62%, the number HHS estimates as currently using electronic storage and retrieval) and all plans will require contractual modification and review by competent legal authority of their business partner contracts. As with the initial development and applicability legal review, we assume providers will use outside legal counsel at an average rate of $125.00 per hour, while plans will use in-house counsel at an average rate of $100.00 per hour. We further assume that a competent legal professional can adjust and review each relevant contract in one-quarter hour per contract.

We further assume that each provider has on average five business partners with whom they share private health information not including health insurance plans.[50] Because relationships between plans and their business partners tend to be more numerous and more complex, we assume that the number of plan contracts proceeds at the rate of (n*(n-1))/2 times the number of provider contracts owing to network effects.[51] Thus, the average plan has 10 business partner contracts requiring review under the proposed rule.[52]

Taking all these facts together yields a cost estimate for providers' business partner contract review of $84.4 million. The cost of business partner contract review for health care plans by comparison is $4.6 million. Together, the costs of requiring business partner oversight are **$89.0 million** initially.

---

[49] Proposed Rule, p. 60025.

[50] These might include two medical laboratories, three professional referral physicians, and one medical payments clearinghouse.

[51] The equation, (n*(n-1))/2, gives the number of connections (i.e., contracts) required to fully connect an "n" sized network.

[52] Given 871,294 providers and 18,225 plans, the average plan serves almost 48 providers. Therefore, our estimates are conservative.

II. On-Going Compliance Costs

A. Patient Records Inspection and Copying (§164.514)

The Department of Health and Human Services estimates that 1.5 percent of patients "encountering" the health care system in a given year will make a request to inspect and/or copy their medical records. HHS, however, fails to distinguish between providers who maintain records in an electronic form (and are therefore subject to the rule) and those who do not, even though HHS estimates that just 62 percent of providers currently process health transactions electronically.[53] Since the proposed rules give patients the right to inspect and copy their medical records regardless of storage medium, a distinction needs to be made between the records stored electronically and those which must be accessed by manual means, since the costs will differ depending on the medium.

HHS relies on a Tennessee hospital-based study that "found an average cost of [providing medical records was] $9.96 per request, with an average 31 pages per request. The total cost of providing copies was $0.32 per page."[54] Further, HHS suggests that non-hospital providers may face lower costs than these, owing to simpler health records. In another study, a health records manager found that in 1992, "The expected time per search was 30.6 minutes; [HHS then suggests] 85 percent of this time could be significantly reduced with computerization."[55] HHS therefore estimates the cost of patient inspection and copying of their records at $81.0 million annually. (8.1 million requests at an average cost of $10.00 per record.)

To evaluate the accuracy of this estimate we make a finer distinction between those offices that provide records electronically and those that do not. We assume that all hospitals maintain patient records electronically and that requests for hospital records will account for roughly 10 percent of all records requested.[56] If retrieval and copying of a manually maintained record takes 30.6 minutes—as the one study cited by HHS found—and 38 percent of non-hospital medical records are kept manually, we estimate that the cost of providing manual records is $37.5 million,[57] if 1.5 percent of all encounters with health care providers result in a records inspection request.

If the HHS claim that electronic storage and retrieval of records cuts the time required by 85 percent, then the average non-hospital request would take 4.59 minutes. At an hourly rate of

[53] Proposed Rule, pp. 60005-60006.

[54] *Ibid*., p. 60016. The Tennessee study was conducted at hospital.

[55] *loc. cit.*

[56] According to the HHS data on health care encounters, hospitals accounted for 20 million encounters in 1996, while ambulatory (non-hospital) encounters were 200 million. (*Ibid*., p. 60016). Thus, we assume a rough proportionality in the volume of requests will obtain.

[57] This assumes an hourly rate for Offices and Clinics of Doctors of Medicine of $26.51. Average wage rates are found by dividing the SIC Code employment into SIC Code payrolls. Physicians' Offices are SIC Code 8010 and hospitals are 8060.

$26.51, the cost to non-hospital health care providers of serving 4.52 million electronic requests equals $9.2 million.

Given that hospital records are on average three times larger than non-hospital records, we assume that the time to process patient requests for hospital records rises proportionately to 13.77 (i.e., 4.59 × 3) minutes per request. At an average hourly cost of $14.81 and assuming these requests constitute 10% of all requests, gives an expected annual cost to hospitals of $2.7 million to satisfy patient requests for their medical records.

In sum then, the cost for all health care providers—given the assumptions laid out in the HHS proposed rule—is **$49.4 million** per year. It bears pointing out however, that this estimate, as well as the HHS estimate, hinge crucially on the assumption that 1.5 percent of patient's will request a copy of their medical records.[58]

B. Requests for Amendment and Correction (§164.516)

Of the 1.5 percent of patients who in a given year request to inspect their medical records, HHS estimates that two-thirds may wish to amend or correct those records. HHS further estimates that the potential cost per incidence of amendment or correction may be $75.00. Thus, a total annual cost of $407.0 million obtains if these assumptions are true.

The HHS estimate of cost and quantity is acceptable as a first approximation of likely amendment and correction costs.[59] However, we also analyze the costs if a different percentage of patients choose to exercise their amendment rights. If just half of those who initially inspect their records request amendment, annual costs of $303.8 million can be expected. If all who inspect subsequently request amendment and/or correction, then annual costs rise to $607.5 million.

These estimates hinge on the initial estimate that 1.5 percent of patients will request inspection of their records. If this estimate is too low by just one percentage point (i.e., 2.5% versus 1.5%), then the estimates for inspection and copying plus the costs for amendment and correction rise by 67 percent. Our best estimate of amendment and correction costs is **$405.0 million.**

[58] We do not have an alternative means of checking the 1.5 percent figure, but we do suggest that a potential approach may be found by considering experiences of credit rating agencies. Americans are able, under the *Fair Credit Reporting Act*, to request copies of their credit records from the reporting and compilation companies. The number who request credit records might form the basis for a good approximation of those who might request medical records. Unfortunately, we have been unable to uncover this data yet, and so we simply offer the method as a potential means of checking this important assumption.

[59] A mathematical error may have entered the HHS estimate of $407 million. If two-thirds of the 1.5% request amendment and/or correction, then 5.4 million records will require some attention at a cost of $75 per incident. 5.4 million times $75 is $405 million, not $407 million.

C. Patient Authorizations for Non-standard Releases of Information (§164.506 [c] [1])

HHS estimates that one percent of 540 million health care encounters will result in requests to withhold the release of protected information for other than payment or treatment purposes. They also estimate that the costs of implementing and honoring these requests will average $10.00 per request. Thus, HHS estimates that the cost of processing patient requests to withhold information will average $54.0 million per year.

Assume, as a first approximation, that the cost of implementing and honoring patient requests to withhold information is $10.00 per request. However, the percentage estimated by HHS who might be expected to do so seems disproportionately low. Elsewhere, HHS suggests that roughly 17 percent (one in six) patients are already taking unusual steps to protect their privacy "including providing inaccurate information, frequently changing physicians, or avoiding care."[60] Seventeen percent therefore, seems a better estimate of those who are likely to restrict access to their medical records and thus to avail themselves of this new right under the proposed rule.

If one in six patients who encounter the US health care system opt to restrict access to their records, providers and plans can expect to process 90 million requests in an average year. At an average cost of $10.00 per incident, the total expected cost per year rises to $900.0 million to implement this aspect of the proposed rule. Moreover, to illustrate just how quickly these costs can spiral out of control, if just one in five patients were to request that information be withheld, the costs of servicing all those requests would rise to $1,080.0 million. In the interests of providing a conservative estimate, assume the midpoint between 1 percent and 16.67 percent of patients (i.e., 8.83%) will restrict access to their records. This assumption generates a median estimate of **$477.0 million**.

D. Ongoing Dissemination of Privacy Policies and Changes Thereto (§164.512)

As we discussed above in the determination of start up costs, after the initial notification in year one, and assuming similar patterns of insurance and system encounters—and assuming 3% annual growth in each category—the ongoing costs of disseminating notices under the proposed rule equate to $17.1 million in year two, $17.6 million in year three and so on.

E. Periodic Re-Training of Personnel on Policies (§164.518)

With regard to ongoing training costs, we assume that plans and providers will simply conduct periodic re-training on a three-year basis in order to remain compliant with the proposed rule. In other words, costs for ongoing training of personnel will average $39.0 million per year.

[60] Proposed Rule, p. 59920.

F. Periodic Review and Oversight of Business Partner Compliance (§164.506 [e])

HHS did not furnish estimates for the ongoing costs of monitoring business partner compliance with respect to protected health information. However, the proposed rule requires that, "a covered entity would be responsible for assuring the each such implementation standard [for ensuring privacy of protected health information] is met by the business partner. … We are proposing that covered entities be accountable for the uses and disclosures of protected health information by their business partners. A covered entity would be in violation of this rule if [it] knew or reasonably should have known of a material breach of the contract by a business partner and it failed to take reasonable steps to cure the breach or terminate the contract."[61]

Since the rule is unclear regarding what constitutes a reasonable steps to ensure business partner compliance this aspect of the rule is particularly difficult to quantify. It may be that contractual terms stipulating privacy protection among business partners may be sufficient. In the extreme case however, direct oversight including periodic audits may be in order. We have presented the most conservative case: i.e., that of zero on-going oversight costs. In other words, these costs are assumed to have been covered in initially establishing a contract terms between business partners (i.e., in the start-up costs).

[61] *Ibid*., p. 59949.