MERCATUS CENTER

GEORGE MASON UNIVERSITY

REGULATORY STUDIES PROGRAM

Public Interest Comment on

Standards for Privacy of Individually Identifiable Health Information[1]

The Regulatory Studies Program (RSP) of the Mercatus Center at George Mason University is dedicated to advancing knowledge of the impact of regulation on society. As part of its mission, RSP conducts careful and independent analyses employing contemporary economic scholarship to assess rulemaking proposals from the perspective of the public interest. Thus, this comment on the Department of Health and Human Service's Standard for Privacy of Individually Identifiable Health Information[2] does not represent the views of any particular affected party or special interest group, but are designed to evaluate the effect of the Agency's proposals on overall consumer welfare.

The comment period on the Notice of Proposed Rule Making (NPRM) in connection with the Department's proposed privacy standards closed on February 17, 2000. On December 28, 2000, HHS issued the final version of this medical privacy rule.[3] Selected differences between the standards, definitions, and requirements in the NPRM and the final rule may be found in Appendix I. Mercatus submits this comment in response to a request made by HHS Secretary Thompson on February 28, 2000 for any additional comment before the rule's final adoption.

Our comment on the final rule contains two sections. The first section compares estimates of the proposed rule's costs to cost estimates for the final rule and discusses selected differences between the two. The second section discusses the benefits that HHS expects to accrue under the rule

I. Cost Estimate Differences

Table 1 summarizes the startup cost estimates (in millions of dollars) for the privacy rule, as estimated by HHS and Mercatus for both the proposed and final rules.

---

[1] Prepared by Jay Cochran, Research Fellow Regulatory Studies Program. This comment is one in a series of Public Interest Comments from Mercatus Center's Regulatory Studies Program and does not represent an official position of George Mason University.

[2] See, "Standards for Privacy of Individually Identifiable Health Information; Final Rule," *Federal Register* 65 (250), pp. 82461-82829.

[3] Because of a delay presenting the final rule to Congress, the effective date of the rule is April 14, 2001.

TABLE 1
MEDICAL PRIVACY RULE ESTIMATED START UP COSTS
($ in Millions)

Privacy Rule Requirement	Proposed Rule		Final Rule	
	HHS	Mercatus	HHS	Mercatus
Initial Legal Analysis	$ 395.0	$ 686.0	$ 597.7	$ 421.4
Policy Development & Documentation		609.9		325.7
Policy Dissemination	105.9	67.9	50.8	68.6
Update Computer Systems	90.0	393.3	261.5	725.5
Personnel Training in Privacy Policies	22.0	116.9	287.1	245.3
Business Associate Contracting	N/E	89.0	299.7	374.1
Minimum Necessary Standard	*Not originally estimated under the proposed rule's standards.*		926.2	619.1
Patient Consent Forms			166.1	166.1
De-Identification of Private Information			124.2	124.2
Self-Insured Health Plans			52.4	52.4
Internal Complaint Procedures			6.6	6.6
Requirements on Research			40.2	40.2
Designate Privacy Officials			723.2	807.5
Inspection, Copying, & Amendment			6.3	6.3
TOTAL Estimated Start-Up Costs	**$ 612.9**	**$1,963.0**	**$3,542.0**	**$3,983.0**

In response to the comments it received following the NRPM, HHS added new cost categories and was better able to quantify its estimates of the economic impact of the final rule.[4] Added categories or those that saw their estimates change significantly included:

- **Initial Policy Analysis, Development, and Documentation** (HHS cost estimate increased while our estimate decreased—both changes arose from improved estimates of input costs.)
- **Computer System Modifications and Disclosure Tracking** (Estimates increased in the final rule owing to better information regarding the systems likely to require modification.)

[4] All HHS cost estimates are taken from Table 1, "The Cost of Complying the Proposed Privacy Regulation" that appears on p. 82761 of the December 28, 2000 *Federal Register*. 45 CFR Parts 160 and 164.

- **Business Associate Contracting** (HHS did not estimate this cost in the NPRM, and our revised higher estimate under the final rule reflects improved information HHS obtained from comments it received in response to the NPRM.)
- **Designation of Privacy Officials** (Cost was not estimated in the NPRM nor in the original Mercatus comment.)
- **Establishing the "Minimum Necessary" disclosure standard** (Cost was not estimated in the NPRM nor in the original Mercatus comment.)

Comparing the original HHS cost estimates made in the NPRM with its more extensive final rule estimates, shows its estimates of start-up costs increasing from an estimated $613 million to more than $3.5 billion—or nearly six-fold. Our estimate of start up costs, by comparison, increased from $2.0 billion under the proposed rule to approximately $4.0 billion under the final rule. With respect to on-going costs, HHS estimates went from about $650 million per year, to $1.6 billion per year in the final rule. Our estimates of the recurring costs owing to the rule went from $987 million to $1.8 billion. A summary of recurring annual costs due to the rule appears in Table 2.

TABLE 2
MEDICAL PRIVACY RULE ESTIMATED ON-GOING COSTS
(Dollars in Millions)

Privacy Rule Requirement	**Proposed Rule**		**Final Rule**	
	HHS	Mercatus	HHS	Mercatus
Records Inspection & Copying	$ 81.0	$ 49.4	$ 1.7	$ 4.9
Amendment & Correction Requests	407.0	405.0	8.2	9.6
Patient Authorizations	54.0	477.0	0.0	0.0
Periodic Policy Notifications	83.4	17.0	37.8	44.0
On-going Personnel Training in Policies	22.0	39.0	50.0	81.8
Business Associate Contracting	N/E	N/E	55.6	124.7
Minimum Necessary Standard	*Not originally estimated under the proposed rule's standards.*		536.7	720.1
Patient Consent Forms			6.8	6.8
De-Identification of Private Information			117.0	117.0
Self-Insured Health Plans			0.0	0.0
Internal Complaint Procedures			10.7	10.7
Disclosure Tracking			95.9	131.1
Requirements on Research			60.5	60.5
Designate Privacy Officials			575.8	533.6
TOTAL Estimated Start-Up Costs	**$ 647.4**	**$ 987.4**	**$1,556.7**	**$1,844.8**

In part, the differences between the proposed and final estimates emerge from a refinement of the existing estimates made in response to the NPRM. In part, the differences also emerge from the addition of new cost categories. The differences between the HHS and Mercatus estimates on the other hand, result, in part, from the adoption of different estimating methodologies, and in part from the effects the rule is assumed to impart on unit costs and quantities in each case, and in turn how these effects are expected to change with time. Significant differences between the proposed and final rules' cost estimates—as well as between HHS and Mercatus estimates—are discussed in further detail in Appendix II.

A. Calculating the Present Value of Privacy Rule Costs

HHS calculates the present value of its cost estimates (recurring plus start-up) at roughly $11.8 billion. It was not possible to replicate the HHS calculation with the costs it presented in Table 1, nor with varying combinations of discount rates. This is most likely due to an unknown difference in the assumed timing of the cash flows. (However, there also appears to be a typographic error in the start up cost estimate column. The reported total by HHS is $3,242 million, but adding the HHS figures produces a sum of $3,542 million.)

Discounting the HHS annually recurring cost estimates of $1.6 billion at the OMB standard rate of 7 percent (over the 10 year horizon assumed by HHS), and then adding the estimated $3.5 billion in start-up costs yields a present value of the HHS cost estimates of $13.0 billion. Conducting a similar calculation on the Mercatus cost estimates yields a present value estimate of $15.2 billion.

Although a 10-year time horizon may be long enough to capture a good portion of the long-run costs of the privacy rule (since at a 7 percent discount rate, 10 years is half of forever), a more complete baseline can be estimated by adopting an indefinite time horizon. That is, assuming the privacy regulation will continue into the indefinite future (a reasonable assumption for most regulations), means we can treat the cost estimates as perpetuities. Using this assumption, the HHS cost estimates yield a long-run baseline cost for the privacy rule of $25.8 billion. Our cost estimates, by comparison, place this figure at $30.3 billion.[5]

Laying aside the differences in cost estimating methodologies and data sources, and regardless of which estimates ultimately prove closer to fact, a question that must also be addressed is whether the privacy protections afforded by the rule are worth a present expenditure of roughly $25 billion to $30 billion? That is, do the benefits to society (i.e., the increase in social welfare) that the rule confers justify the costs expected to obtain under the rule?

[5] Adding the discounted costs to federal state and local governments (as estimated by HHS) raises the discounted cost of the privacy rule to between $31.5 and $36.1 billion respectively.

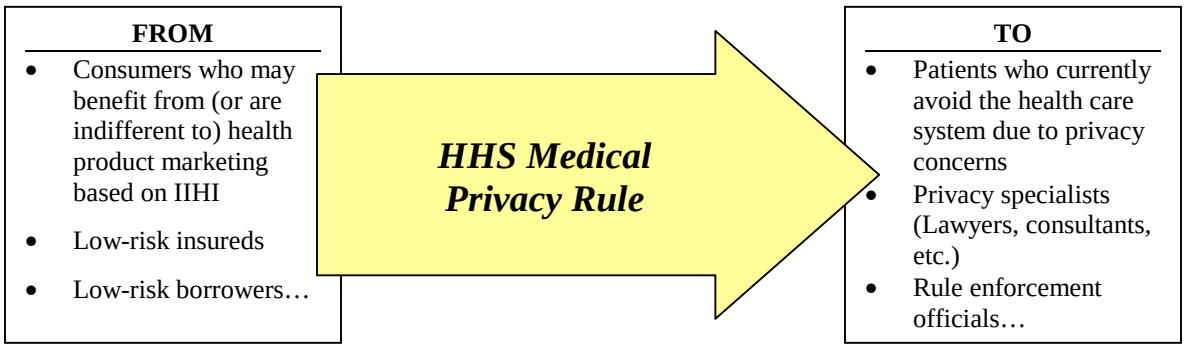
II. Benefits Attributed to the Rule

In building its case for the benefits of the privacy rule, HHS reports on a Harris-Equifax survey that found seven percent of respondents did not seek services for physical or mental health conditions due to fears about job prospects or other opportunities.[6] HHS also cites a 1999 report that claims "many people fear their personal health information will be used against them to deny insurance, employment, and housing, or to expose them to unwanted judgments and scrutiny."[7]

No doubt, HHS accurately relates the facts in these reports. However, HHS fails to consider that "unwanted judgment and scrutiny" is the obverse of the ability to price risk accurately. In other words, if HHS wishes to use increases in access to the health care system (in response to increased privacy protections) as a partial proxy for the benefits of the rule, then it must also include as an offsetting cost, the increase in risks (i.e., losses) that are likely to result from an impaired ability to price risks accurately in insurance underwriting, credit applications, or employment screening.

In fact, the potential benefits that HHS does ascribe to the rule actually represent transfers from one segment of society to a segment that currently avoids the health system because of perceived poor privacy protections. It is likely true that those individuals who currently avoid the health care system due to perceived poor privacy protections will benefit from the transfers the rule directs their way. However, the question at issue here is whether society as a whole benefits from the rule and its attendant costs and transfers? That is a much tougher determination to make and requires an ability to judge the relative value of the transferred resources—i.e., the value to those from whom the resources are taken, as well as the value of the transferred resources to those whom they are given. HHS attempts to calculate the latter, but completely ignores the former. It therefore incorrectly treats transfers as benefits by failing to consider the offsetting values of the person from whom such transfers are taken. Figure 1 schematically depicts the transfer mechanism that is likely to result from the rule's imposition.

FIGURE 1
SOME LIKELY TRANSFERS RESULTING FROM THE MEDICAL PRIVACY RULE



[6] See the Final Rule, p. 82777.

III. Conclusion

Even laying aside the question of transfers versus net societal benefits, in its final form, the medical privacy rule is complex and, in some cases, either redundant or inconsistent. The rule is redundant, for instance, in the sense that it mandates consent even though consent is customarily obtained today without the rule; or redundant in that it mandates patients' ability to inspect, copy, or amend their medical records even though most plans and providers already allow this practice without the rule. The rule is inconsistent in the sense that it purports to protect patient privacy, but is then riddled with exceptions such as those for certain marketing or fund raising purposes. When the inconsistencies and redundancies are combined with the observation that many of the rule's purported benefits are in reality transfers rather than net increases in social welfare, one can expect the likely long-run effect of the rule will be that it becomes another albatross on an already heavily regulated part of the US economy.[8]

[7] *ibid*., p. 82776.

[8] Our comments on the medical privacy rule should not be construed as in any way disparaging of the motives of the regulators at the Department of Health and Human Services. We understand that promulgation of the privacy regulations was required by operation of law (specifically, Public Law 104-191, *Health Insurance Portability and Accountability Act*, enacted August 21, 1996). However, when Congress delegates its legislative authority with vague directions and through a default mechanism—as it did in the HIPAA legislation—it should not be surprising that the emergent regulations tend to be costly inasmuch as regulators face different incentives and constraints than legislators do.

APPENDIX I

SELECTED DIFFERENCES BETWEEN PROPOSED AND FINAL
STANDARDS TO PROTECT PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION
As Promulgated by the Department of Health and Human Services

PROPOSED RULE	**FINAL RULE**	**COMMENT ON CHANGE**
	Consent and Authorization	
No consent required for use or disclosure of protected information in connection with treatment, payment, and health care operations.	Health care providers with direct treatment relationship must obtain a signed consent and provide notice that details the provider's health information practices Providers may condition treatment on receipt of a signed ***consent*** form. (82511)	Less restrictive in the proposed form. Health care plans and providers already routinely gather patient consent and so the change is arguably superfluous.
Covered entities were prohibited from seeking individual consent before treatment.	Consent required in final rule.	Preserves current modes of operation.
No *authorization* required in cases of public policy, safety, and health.	Same.	No change.
Individuals may restrict access or disclosures by health care providers.	Individuals may seek restrictions of all covered entities, not just health care providers. (164.522)	Increases scope of rule.
Patient authorizations required for fund raising based on IIHI.	Fund raising for the covered entity's own benefit is exempted.	Weakens protections in the name of charity fundraising.
Patient authorizations required for marketing	Certain marketing functions exempted from	Dilutes privacy protections against

programs based on IIHI.	having to obtain prior authorization.	unwanted solicitation.
Business Partner Oversight Requirements		
Disclosures to business "partners" required a written contract that would limit the use and disclosures permitted to the partner.	Contracts specifying privacy protections among business "associates" still required.	Change in terminology used, but not in standard.
Covered entities must take action when they know, *or should have known*, about a business partner's violation of the rule's requirements.	Covered entities are responsible now, only when they know of a pattern of activity that constitutes a breach of the contract. "Should have known" standard removed from final rule.	Somewhat less onerous.
Covered entities must regularly monitor and ensure privacy protection by its business partners.	This requirement eliminated, except to extent that covered entities must actively investigate and document credible evidence of a violation by a business partner.	Less onerous.
Business associate must return or destroy all protected health information received from a covered entity when business relationship is terminated	Business associates must return or destroy all protected information when feasible and lawful.	In the proposed form, regulation would have hampered audit and other record keeping functions.
Research Using Health Information		
Research requires either authorization from the subjects, or a waiver that passes through a review board process.	If only de-identified health information is used, protected health information can be used in research.	Less onerous.
Definitions		

Covered entities must describe in plain language the uses to which protected information are put; distinguishing between those required by law, and those permitted but not required by law.	Covered entities must describe all uses and disclosure of protected health information that they are permitted or required to make under the rule.	Final requirement may have the effect of over-supplying the subject with information as to how their IIHI may be used.
"Protected Health Information" means "individually identifiable health information that is or has been electronically maintained or transmitted by a covered entity…"	Expanded to include all individually identifiable health information maintained by a covered entity regardless of form.	Now paper records as well as computer records are covered.

APPENDIX II

COST ESTIMATE DIFFERENCES BETWEEN PROPOSED AND FINAL MEDICAL PRIVACY RULES

1. Initial Policy Analysis, Development, and Documentation

Mercatus originally estimated these aspects of the privacy rule to result in start-up costs of roughly $1.3 billion. Using the same methodology (see Appendix of original comment for more extensive discussion of the estimate methodologies), but changing the hours assumed necessary for these tasks to parallel the assumptions made by HHS in the final rule cost estimates, produces a revised start up cost estimate for Privacy Policy Analysis, Development, and Documentation of $746 million.

HHS, by comparison, estimated these combined costs of analysis, policy development, and documentation at $395 million and $598 million in the proposed and final rules respectively. HHS may be misplacing its optimism on how much of individual firm policies can be implemented from boilerplate policies developed by professional associations. Given the high penalties associated with violations of the rule, prudent risk management argues in favor of larger investments in legal review up front.

Our estimates assume that health care providers (doctors, hospitals, etc.) will incur just eight hours of labor opportunity costs (legal fees, diverted management time, etc., or about one business day) developing its privacy policies. This estimate may prove quite conservative given that this is a fairly complex set of rules, exceptions, and standards with which to comply. We also estimate that health care plans will (given generally larger and more complex operations) incur about a workweek's worth of costs to analyze, develop, and document privacy policies that comply with the requirements of the rule.

2. Computer System Modifications (Disclosure Tracking)

The rule requires that plans be able to track who has accessed individually identifiable health information, and to implement safeguards on such systems to prevent impermissible disclosures. We estimated that to install software audit trails (in the 62 percent of firms who use electronic record keeping systems, see NPRM), institute password protected files, limit access to certain files or directories, and to implement the "minimum necessary" disclosure standard as relates to computer systems will generate costs in the computer systems area of $725 million. This revised estimate uses the same methodology as in the original but the additional costs of modifying computer systems to support the minimum necessary disclosure standard added $332 million to our original $393 million estimate.

The Department by contrast estimates that the Disclosure Tracking system (i.e, audit trails, security, etc., but not "minimum necessary") will account for $262 million in estimated start up costs. HHS places the costs for computer systems changes related to implementing the minimum necessary standard in with the other costs expected to result from minimum necessary. If the HHS minimum necessary computer costs equal roughly $300 million, then the equivalent HHS cost estimate for computer systems modifications required on account of the rule will be somewhere in the vicinity of $560 million in the first year.

3. Business Associate Contracting,

Mercatus had originally anticipated that the requirements for business partner contracting would be nominal changes to existing contracts, and that competent lawyers could draft such changes in short order (i.e, in about one-quarter hour, on average). Consequently, our original start-up cost estimate for this aspect of the rule was $89.0 million. HHS however, suggests that one hour for providers and two hours for health plans might be more accurate. Using these longer time assumptions, generates a revised estimate of $374 million, versus an HHS estimate of $299.7.[9]

HHS could not quantify the costs of business associate contracting in its original cost estimate. In the final rule, moreover, HHS removed the requirement that plans and providers conduct periodic oversight (e.g., through audit) of the privacy practices of their business partners (referred to as "associates" rather than partners in the final rule).

4. Designation of Privacy Officials

Health care plans and providers must appoint or hire an employee to act as privacy ombudsman within the firm. Although the department anticipates that this duty would fall to an existing employee in most cases, the requirement nevertheless represents a diversion of resources that are costs of the rule. Using the number of hours and the hourly rates suggested by HHS in the final rule, we estimate the privacy official requirement will generate start up costs of $808 million and annually recurring costs of $534 million. HHS by comparison, estimates these costs at $723 million and $576 million respectively.

5. Establishing the "Minimum Necessary" disclosure standard.

In the original cost estimates, we assumed that the minimum necessary disclosure standard would not be a significant departure from current practice. In part, the Department, agrees and in part it disagrees with this assumption. It states in the final rule for example, that, "…the Department has concluded that the requirements of the final rule are generally similar to the current practice of most providers."[10] It goes on to say though, that "Under the final rule, we anticipate providers will have to be more thorough in their policies and procedures and more vigilant in their oversight of them; hence, the costs of this provision are significant."[11]

Based on this analysis, we estimate the start up costs associated with establishing minimum necessary disclosure standards at $619 million. HHS, by contrast, places these costs at $926 million (See the discussion above on "Computer Systems Modifications" for an explanation of the principal differences here.) We estimate the on-going costs associated with managing the minimum necessary standard at $720 million per year. HHS places these annually

[9] The remaining differences are attributable to slightly different hourly rates assumed, and the number of business partners with whom each plan and provider is assumed to have a business relationship.

[10] See *Final Rule*, p. 82767.

[11] *ibid*., p. 82767.

recurring costs at $527 million. The chief difference owes to an estimate on our part of the possible volume of non-routine requests for individually identifiable health information that will require case-by-case review—a cost that HHS did not factor in its estimates of the final rule's costs.

6. Governmental Costs

HHS provides estimates of the costs it expects federal, state, and local governments to incur once the rule is effective. These costs largely arise out of each level of government's role as either a health care plan or provider. It is debatable whether such estimates are appropriately classified as costs. Transfers from the consumers and suppliers of health care services to the government might be the more accurate classification. In any event, HHS places federal government start up "costs" because of the rule at $196 million, and recurring federal privacy rule costs at $160 million. HHS estimates State and local government start up costs at $460 million and recurring state and local costs at $194 million.

Appendix III
RSP Checklist

Standards for Privacy of Individually Identifiable Health Information

Element	Agency Approach	RSP Comments and Grades
1. Has the agency identified a significant market failure?	HHS identifies what it believes to be a market failure. It claims, "The incentives facing a company that acquires individually identifiable health information also discourage privacy protection. …A company gains the full benefit of using such information … however, [it] does not suffer the losses from disclosure of protected health information." (p. 82761) **Grade: D**	To suggest a market failure presupposes poorly defined or weakly defensible property rights. HHS makes a combination claim of externality (companies reap the benefits but do not bear the costs) and asymmetry (i.e., high monitoring costs for subjects). However, the Courts have long placed property rights in this information in the collectors (MDs, hospitals, etc.). There is no *a priori* reason to suspect the incentives must run in the direction HHS supposes, and in fact, the constraints of professional ethics, respect for patients' wishes, and indeed profit and loss run against this supposition.
2. Has the agency identified an appropriate federal role?	HHS suggests there is an appropriate federal role in establishing baseline protections and instilling uniformity across states. **Grade: B**	While there may be some benefits that flow from uniform standards, there are also losses that result from foregone experimentation that could have occurred at the state level.
3. Has the agency examined alternative approaches?	The Agency does consider some alternatives within the framework of a prescriptive federal rule. **Grade: C**	HHS does not consider, however, alternative property rights arrangements in information, other than vesting them in the individual subject.

Element	Agency Approach	RSP Comments and Grades
4. Does the agency attempt to maximize net benefits?	HHS identifies what it believes to be benefits—in the form of people returning to the health care system who were previously avoiding it due to perceived lax privacy protections. **Grade: D**	The benefits to these (avoiding) individuals are more accurately accounted for as transfers from those who benefit from more accurate health care information (e.g., low risk insureds) to those who prefer to shield their health information from disclosure.
5. Does the proposal have a strong scientific or technical basis?	HHS draws inferences about the benefits of the rule from unconstrained polling data. It rests its benefits analysis on a very weak scientific foundation. **Grade: D**	HHS should instead consider how patients and providers are currently operating with respect to privacy. In several instances in fact, the rule simply codifies existing practices (e.g., consent forms, the ability to copy and inspect records, etc.) and is therefore superfluous.
6. Are distributional effects clearly understood?	HHS does not actively consider distributional effects. **Grade: F**	The misidentification of transfers as net benefits (see 4 above) is one indication that HHS does not clear understand the distributional effects stemming from its rule.
7. Are individual choices and property impacts understood?	HHS, through this rule, changes the existing property rights arrangements in medical information. **Grade: F**	HHS fails to consider that walling off private medical information behind individual patient consent may lead to less accurate pricing of risks and therefore to transfers of property from less risky members of society to society's more risky members. In the short run, this rearrangement is likely to prove disruptive as people adapt. In the long run, it may also prove to be less efficient arrangement as well.
