Annals of Health Law

Volume 9
Issue 1 *2000*

Article 3

2000

A Critical Analysis of Health and Human Services' Proposed Health Privacy Regulation in Light of the Health Insurance Privacy and Accountability Act of 1996

A. Craig Eddy
University of Montana

A Critical Analysis of Health and Human Services' Proposed Health Privacy Regulations in Light of The Health Insurance Privacy and Accountability Act of 1996

*A. Craig Eddy**

INTRODUCTION

Historically, Americans have zealously protected their privacy and personal information.[1] The more intimate the information, the greater the level of concern. The reason Americans cherish privacy so dearly is perhaps rooted in their devotion to personal freedom and individual identity. Authors Ellen Alderman and Caroline Kennedy capture this feeling in their book *The Right to Privacy* by writing:

> Privacy covers many things. It protects the solitude necessary for creative thought. It allows us the independence that is part of raising a family. It protects our right to be secure in our own homes and possessions, assured that the government cannot come barging in. Privacy also encompasses our right to self determination and to define who we are. Although we live in a world of noisy self-confession, privacy allows us to keep certain facts to ourselves if we so choose. The right to privacy, it seems, is what makes us civilized.[2]

Facts regarding physical and emotional wellbeing in the form of a medical record are perhaps the most intimate and personal

* Associate Professor of Cardiovascular Disease, Department of Pharmaceutical Sciences, and Adjunct Professor of Law, University of Montana; Vice President, St. Patrick Hospital, Missoula, Montana; Of Counsel to the firm of Garlington, Lohn and Robinson, Missoula, Montana; A.B., Oberlin College, 1974; M.D., University of Cincinnati, 1978; J.D. University of Montana, 1999; LL.M. 2000 Loyola University of Chicago. The author would like to thank Professors John Blum, Joan Krause, Ida Androwich and Larry Singer for suggestions on earlier drafts of this paper; Dr. Margaret Eddy for editorial assistance and other support; Professors Charles Rice and Vern Grund for unfailing support; Elizabeth Lantz, Carla Hirsen and the editors of The Annals of Health Law for their helpful suggestions; and of course Ben, Matt and Zach who make my life enjoyable and worthwhile.

1. *See* DARIEN A. MCWHIRTER & JON D. BIBLE, PRIVACY AS A CONSTITUTIONAL RIGHT 9 (1992) (giving several examples of how Americans have been much more concerned with privacy than their European ancestors).

2. ELLEN ALDERMAN & CAROLINE KENNEDY, THE RIGHT TO PRIVACY xiii (1995).

of all information. A medical record consists of information divulged by a uniquely vulnerable human being, worried in some manner about the core of her very existence, to a trusted person with superior knowledge. This data is recorded after being filtered through the critical lens of a physician or other caregiver ostensibly encumbered by no interest beyond the patient's health and well-being.

Patients always have been concerned that information entrusted to their physicians is not revealed to others and possibly used against them. Anglo-American courts recognize the need to balance the societal interest in encouraging patients to be completely open and truthful with their physicians against the need for society to access certain health information. This has taken the form of a formal judicial policy of a patient/physician privilege which parallels the sanctity of the nearly two thousand year old penitent/confessor privilege.[3]

The origin and development of extensive recorded medical information is actually quite new. Until recently, medical records were minimalist notes jotted quickly by a physician to remember a few details of a patient's condition that he feared he might forget along with perhaps some billing information. Most of the details, especially the intimate ones, resided primarily in the head of the physician. In the period after World War I, physician specialization proliferated and was attended by an increase in the practice of patient referral. This basic concept was expanded during World War II where wartime medicine evolved from definitive treatment on the front lines, to initial battlefield first aid, followed by transport and ultimate treatment at behind-the-lines field hospitals. In this model of patient care, it became imperative for physicians to not only remind themselves about care delivered and treatments instituted but also to com-

3. *See* Seymour Moskowitz & Michael J. DeBoer, *When Silence Resounds: Clergy and the Requirement To Report Elder Abuse and Neglect*, 49 DEPAUL L. REV. 1 (1999). "The clergy-penitent testimonial privilege has its roots in ancient English common law, and its antecedents may be found in Roman Catholic doctrine that considered the Seal of Confession inviolate. The privilege was first recognized in the United States by a New York court in 1813 which held that a Catholic Priest could not be compelled to reveal what he heard during confession. The court found that forcing a priest to violate the secrecy of the confessional violated the priest's constitutional right to the free exercise of religion. As early as 1875, in dictum, the Supreme Court stated: 'On this principle, suits cannot be maintained which would require a disclosure of the confidence of the confessional: . . . .' Today, all American states and the federal courts recognize a clergy-penitent privilege, although its scope varies from jurisdiction to jurisdiction." *Id.* at 55-56.

municate that treatment to other subsequent caregivers. Finally, with the explosion in medical technology over the past twenty years there has been a concomitant increase in specialization and, in some cases, delegation of medical treatments to non-professional technicians. These advances in medical care spawned a corresponding increase in the amount of information formally recorded so it can be accurately and efficiently communicated to multiple users over longer distances. Thus, as the norm of medical care has evolved from delivery by a single physician in a single location, to care rendered by a multidisciplinary team often located on diverse campuses and even in different states, the meticulously detailed, problem-oriented medical record[4] has become an indispensable tool to coordinate, document and streamline care.

Traditionally, physicians have been stalwart guardians of the personal medical information revealed to them. That duty has been explicit and implicit for more than two thousand years, emblazoned in both the Hippocratic Oath[5] and the Code of Maimonides,[6] two of the oldest statements of physician commitment to patient privacy. These statements are still recited at medical student graduations and hang in physician offices throughout the country as a reminder of that duty.

Physicians originally fulfilled their duty to guard patient privacy by insisting that patient medical records were a physician's

4. The universally accepted protocol for individual encounters described in medical records divides the narrative into four parts, using the acronym SOAP (Subjective, Objective, Assessment, Plan), which was introduced to medicine in the late 1960s along with the concept of the problem-oriented medical record. Subjective means what the patient says about herself or her condition, while objective means what physicians and other providers find on examination. Assessment is the physician's subjective medical judgment about what is transpiring with the patient; plan outlines the proposed course of action and intervention. *See generally* William J. Donnelly & Daniel J. Brauner, Comment, *Why SOAP is Bad for the Medical Record*, 152 ARCH. INTERNAL MED. 481 (1992); *see also* John D. Stoeckle & J. Andrew Billings, *A History of History-taking: The Medical Interview*, 2 J. GEN. INTERNAL MED. 119 (1987).

5. "Whatever, in connection with my professional practice or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret." Hippocratic Oath, circa 400 BCE, reprinted in HIPPOCRATES, WORKS 299-301 (trans., Loeb).

6. "Inspire me with love for my art and for Thy creatures. Do not allow thirst for profit, ambition for renown and admiration, to interfere[through misuse of medical information] with my profession, for these are the enemies of truth and of love for mankind and they can lead astray in the great task of attending to the welfare of Thy creatures." Attributed to Moses Maimonides, a twelfth-century Jewish physician in Egypt, but possibly written by Marcus Herz, a German physician, pupil of Immanual Kant, and physician to Moses Mendelssohn. First appeared in print in 1793.

work product and, thus, actually a physician's property. With this view, they adamantly refused to let patients themselves examine those records except under extenuating circumstances. As medical paternalism declined after World War II, patients were given the right to access their own information. However, perhaps even as an unintended consequence, the derivative right of the patient to assign access to his medical records to third parties—such as relatives, attorneys and insurance companies—accompanied the right of personal access to medical records.

Unfortunately, patients are proving less successful at protecting their own medical information than their physicians once were. Third party payers, managed care providers and the government increasingly are interested in the personal medical information of patients for whom they underwrite medical expenses. These parties argue that they have a legitimate business need for such information and then insert that claim into the language of a contract with the patient. Additionally, employers, life insurance companies and marketing interests are attempting to claim an expanded interest in individual patient information. This claim is more tenuous, but colorable, if its root is in information legally purchased from another legitimate owner or information resident on shared informatics systems.

These third party claims to information generated in the physician patient relationship have resulted in patients losing control over their individual medical information once it enters the stream of commerce. Anecdotal reports of abuses of personal information, coupled with America's privacy fixation and a growing distrust of the government and large corporations, have stimulated the American public to demand better control over their personal information.

After an extended public outcry voicing the concern that there was less protection for the privacy of medical information than existed for the protection of financial information, Congress, as an afterthought to the main body of the Health Improvement and Accountability Act of 1996 (HIPAA), added section 264 entitled "Recommendations with Respect to Privacy of Certain Health Information."[7] Section 264 of HIPAA, in turn, required Congress or the Department of Health and Human Services (HHS) to safeguard the privacy interests that individual patients were having difficulty protecting.

7. Pub. L. No. 104-191, 110 Stat. 1936 (1996).

This article has several purposes. Its primary purpose is to inquire, through a detailed analysis of all relevant statutory provisions, whether it is likely that the HIPAA legislation or the regulations promulgated thereunder (the "Standards for Privacy of Individually Identifiable Health Information Regulations" (SPIIHI)) will efficiently and cost-effectively defend the privacy issues they were intended to safeguard. Neither the premise that medical information should be considered private nor the premise that it deserves some level of protection is disputed. Rather, this article critically analyzes HHS' broad and expensive proposal to determine whether it is an efficient use of health care dollars. Indeed, compliance with the law is projected to cost health care providers billions of dollars.

To accomplish this critical analysis, an understanding of exactly what aspect of privacy HHS intends to protect and a knowledge of the pervasiveness of the threat to that privacy is necessary. To that end, Part I addresses the concept of privacy in general and, more specifically, medical privacy in our current society. It points out the first major flaw in SPIIHI: the fact that HHS failed to adequately and coherently define its ultimate goal. The article then attempts to define more clearly what aspect of privacy HIPAA and SPIIHI should protect. Part II focuses on the extent of the invasion of medical record privacy that exists currently and may exist in the future highlighting SPIIHI's second major flaw: its proposed protections are not focused on the existing problem.

Parts III and IV examine the privacy section of HIPAA (§264) and HHS's proposed rule (SPIIHI) in detail. Part IV examines how and why Congress acted legislatively to protect the privacy of medical records. Part IV explains how the Department of Health and Human Services has exceeded the legislative mandates of Congress with its six hundred page proposed rule. It briefly discusses all aspects of SPIIHI but focuses on two primary areas: the actual provisions and the regulatory impact analysis. Of particular importance is the comparison of HHS' cost analysis to that of private industry.

Part V analyzes whether HHS' efforts are constitutional, cost efficient, or effective, and concludes that they are not. It also examines the rationale for other major burdens imposed on the health care system by SPIIHI (administrative, preemptive, research related and enforcement related) concluding that these burdens cost more than the value of the protection they offer.

Finally, Part VI proposes three potential courses of action for HHS to salvage its work in SPIIHI, and constitutionally and more cost effectively accomplish its purpose to protect IIHI.

I. THE CONCEPT OF PROTECTABLE PRIVACY: AN HISTORICAL AND CURRENT PERSPECTIVE

A. The Concept of Privacy in General

The notion of a right to privacy is ancient and pervasive. It is alluded to in the Bible and expressed in the Aristotelian concept of a dichotomy between the public and private realms.[8] In more recent history, John Locke applied this concept to distinguish between private property and property owned publicly or in common with all.[9] Anthropologic studies by Margaret Mead and others suggest that the concept of privacy is cross-cultural and present in all but the simplest, most primitive societies.[10]

Americans can never be sure what their founding fathers intended regarding federal protection of a right to privacy. A "right to privacy" is not explicitly mentioned in the United States Constitution or the Bill of Rights. In fact, the word privacy never appears in these documents at all, arguably suggesting that the founding fathers thought the states were capable of protecting citizens' privacy rights as a part of their general welfare. Despite this lack of clarity, both state and federal courts, as well as legislatures, have demonstrated a willingness to protect some forms of personal privacy.[11] The concept of a fundamental right to privacy is bifurcated into two distinct rights: one right is based in natural law,[12] the Judeo-Christian law, Aristotle and Locke's philosophy of law and British com-

8. *See* JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS AND THE RISE OF TECHNOLOGY 9-25 (1997). Ms. DeCew quotes Milton Konvitz pointing out that the Adam and Eve story introduces the feeling of shame at the violation of privacy and emphasizes how Aristotle divided an individual's life into two realms: the polis (the realm common to all citizens) and the oikos (the realm of the private household).

9. *See id.* (citing JOHN LOCKE, THE SECOND TREATISE ON GOVERNMENT 4 (Thomas P. Peardon ed. 1988)).

10. *See id.*

11. *See id.*

12. The right of privacy has its foundation in the instincts of nature. It is recognized intuitively, consciousness being the witness that can be called to establish its existence. Any person whose intellect is in a normal condition recognizes at once that as to each individual member of society there are matters private, and there are matters public so far as the individual is concerned. *See* Pavesich v. New England Life Ins. Co., 50 S.E. 68, 69 (Ga. 1905).

mon law; a second right is implied from the language of the United States Constitution.[13]

B. The Common Law Right to Privacy

The common law right of privacy has been crafted by and enforced through the law of tort, initially using the tort of battery.[14] In 1880, Judge Thomas Cooley included in his treatise on torts a "right to be let alone," which he explained as a "right" to one's person or personal immunity.[15] Soon after, in a medical setting, the term privacy was invoked in a battery tort advanced by a woman who was observed during childbirth without her consent.[16] In this case, the Michigan Supreme Court held: "the plaintiff had a legal right to the privacy of her apartment at such a time, and the law secures to her this right by requiring others to observe it, and to abstain from its violation."[17]

In 1890, Louis Brandeis and Samuel Warren eloquently developed Cooley's tort concept in their Harvard Law Review Article, entitled *The Right to Privacy*.[18] This article has been called the most famous and influential law review article ever written, prompting Roscoe Pound to remark that it " 'did nothing less than add a chapter to our law.' "[19] Brandeis' and Warren's article stated that "political, social and economic changes entail the recognition of new rights"[20] and they proposed, in reaction to a perception that the press was overstepping the bounds of decency, two new rights: the right to be let alone and the right to be protected from the unauthorized publicity of essentially private affairs.[21] They urged the common law to vindicate and protect those rights.[22] They further observed that the common law already offered some protection against the mental distress associated with public publishing of private information (e.g. the protection against making private letters available to the pub-

13. *See* DECEW, *supra* note 8.
14. *See* DECEW, *supra* note 8, at 17.
15. THOMAS C. COOLEY, LAW OF TORTS (1880).
16. *See* De May v. Roberts, 46 Mich. 160 (1881).
17. *See id.* at 165-166 (emphasis added).
18. *See* Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
19. Nicholas D. Bieter, *Minnesota's Right of Privacy Torts: Expanding Common Law Beyond Its Reasonable Constitutional Bounds in* Lake v. Wal-Mart Stores, Inc., 20 HAMLINE J. PUB. L. & POL'Y 177, 181 (1998).
20. Brandeis & Warren, *supra* note 18.
21. Brandeis & Warren, *supra* note 18, at 215.
22. *See id.* at 195-215.

lic).[23] They argued this protection should be extended to protect privacy more generally saying:

> "The principle which protects personal writings and any other productions of the intellect or of the emotions is the right to privacy, and the law has no new principle to formulate when it extends this protection to the personal appearance, sayings, acts, and to personal relations, domestic or otherwise."[24]

They reinforced their argument by reviewing various court decisions that protected privacy and concluded that an individual had a type of ownership interest in the facts of his private life.[25]

Brandeis and Warren conceded their proposed common law right to privacy was not absolute.[26] For example, matters of general public interest or pertaining to public figures could be investigated and published without legal recourse.[27] Further, they stipulated that consent should be a defense to invasion of privacy.[28]

Between 1890 and the present, the tort of invasion of privacy has been recognized in some form, via statutory or common law, by all fifty states.[29] With some state to state variation, it is usually subdivided into four major groups: (1) appropriation of an individual's name or image for the commercial advantage of another; (2) publication of facts placing an individual in a false light; (3) intrusion upon an individual's affairs or seclusion; and (4) public disclosure of private facts about an individual.[30] The first two groups, commercial advantage and false light, have little to do with the type of privacy at issue in medical information and will not be included in this discussion. However, intrusion into an individual's affairs or seclusion and public disclosure of private facts are the type of privacy invasion that occurs when medical records are made public. Further, this is the type of privacy that states have been willing to protect under their reserved power to guard the welfare of their populations. However, in the universe of common law privacy rights, a real

23. *See id.* at 213.
24. *Id.*
25. *See id.* at 195-200.
26. *See* Brandeis & Warren, *supra* note 18, at 213-20.
27. *See id.*
28. *See id.*
29. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 60008. However, four states limit the right of privacy to commercial use violations. *See* JOHN WADE ET AL, CASES AND MATERIALS ON TORTS 948 (1994).
30. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960) (later incorporated into the Second Restatement of Torts).

question remains about whether or not the Federal government should intrude upon this state power.

C. *The Constitutional Right to Privacy*

The second type of privacy right is Constitutional in nature. Constitutional privacy exists at both the state and federal levels. Thus, state and federal protections overlap, with some states affording more privacy protection than the federal government.

1. Federal Privacy Protections

The federal constitutional right to privacy also can be traced back to Louis Brandeis, who, in his role as a Supreme Court Justice, advocated a broad interpretation of the Fourth Amendment to insure that the government refrained from intruding into the privacy of the individual. He stated in his dissent in *Olmstead v. United States*:[31]

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone – the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.[32]

Between 1928 and 1965, Brandeis' position in the *Olmstead* dissent gradually gained favor with the Court and in the1965 *Griswold v. Connecticut*[33] opinion, Justice William O. Douglas found a penumbral right to privacy emanating from the Constitution and its First, Fourth and Fifth Amendments. This concept quickly became accepted and, after *Olmstead* was overturned by *Katz v. United States*[34] in 1967, the right to privacy was cited in a variety of cases over the next few years. However, the citation was always in the context of a right of privacy against govern-

31. 277 U.S. 438 (1928).
32. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J. dissenting).
33. 381 U.S. 479 (1965).
34. 389 U.S. 347 (1967).

mental intrusion, not against the intrusion of an individual or a private corporation into the affairs of a patient.[35]

Although the United States Supreme Court has recognized a right of individuals to be free from governmental intrusion into their private lives, it has not yet held that this right to privacy limits governmental power to collect data about private individuals.[36] In *Whalen v. Roe*,[37] the Supreme Court examined this question in detail and held in the majority opinion that "state legislation which has some effect on . . . privacy" is not unconstitutional "simply because a court finds that effect unnecessary, in whole or in part."[38] However, Justice Stevens noted in dicta that government data collection could threaten individual privacy, and that the right to collect that data could be limited by a duty to avoid unwarranted disclosure.[39] In the end, the Court in *Whalen* specifically refused to decide whether it would uphold a statute without these safeguards saying: "we . . . need not, and do not, decide any question which might be presented by . . . a system that did not contain comparable security provisions."[40]

2. State Privacy Protections

Most states follow the federal lead in deriving a right to privacy from the penumbras of their constitutions. However, ten state constitutions confer to their citizens an explicit right of privacy.[41] Some states, such as California, have added this provision by constitutional amendment.[42] Others, such as Montana, have included the right in the ratified document.[43]

For the most part, state constitutional provisions only protect against governmental intrusion into an individual's privacy.

35. *See* Loving v. Virginia, 388 U.S. 1 (1967) (striking down a Virginia statute forbidding interracial marriage based on a right to privacy); *see also* Stanley v Georgia, 394 U.S. 557 (1969) (allowing the possession of obscene material in the privacy of an individual's home) *and* Eisenstadt v. Baird, 405 U.S. 438 (1972) (citing the right of privacy as a reason to permit distribution of contraceptive devices).

36. *See* JOHN E. NOWAK & RONALD D. ROTUNDA, CONSTITUTIONAL LAW §§ 14.26-14.30 (5th ed. 1995).

37. 429 U.S. 589 (1977).

38. *Id.* at 597.

39. *See id.* at 605.

40. *See id.* at 605-06.

41. *See* DARIEN A. MCWIRTER & JON D. BIBLE, PRIVACY AS A CONSTITUTIONAL RIGHT 174, 179 n.5 (1992) (Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina and Washington).

42. J. Clark Kelso, *California's Constitutional Right to Privacy*, 19 PEPP. L. REV. 327, 328 (1992).

43. MONT. CONST. art. II, § 10.

Some states however, such as Montana, indicate a willingness to extend this protection to non-government actions.[44] Montana's explicit right to privacy says, "[t]he right of individual privacy is essential to the well being of a free society . . . ."[45]

D. How Much and What Kind of Privacy Does SPIIHI Intend To Protect?

In light of the historical context surrounding the right of privacy, the question arises as to the type and scope of privacy protection HHS is seeking to afford. It is unlikely that HHS is referring to commercial advantage and false light privacy protection because these types of privacy protection have little to do with medical records. Therefore the privacy rights HHS is likely referring to are intrusion into an individual's seclusion and public disclosure privacy rights. In support of this supposition, the SPIIHI section entitled "Need for the Proposed Action" quotes liberally from the case of *Whalen v. Roe*[46] making it clear that SPIIHI intends to address only one of many aspects of the privacy right:

> The [Whalen] Court, in upholding the statute, recognized at least two different kinds of interests within the constitutionally protected *zone of privacy*. "One is the individual interest in avoiding disclosure of personal matters," such as this proposed regulation principally addresses. This interest in avoiding disclosure, discussed in *Whalen* in the context of medical information, was found to be distinct from a different line of cases concerning "the interest in independence in making certain kinds of important decisions."[47]

Another issue surrounding HHS' intentions is whether it is referring to common law or constitutional privacy. Although HHS mixes the discussion of these two rights, again, considering the underlying purpose of the regulation, it seems most likely HHS is focusing on the common law type protections because Constitutional privacy protections are too narrow to accomplish its stated goals. However, by invoking the term "fundamental right" and using *Whalen*–a governmental intrusion case–to justify SPIIHI's burdens, HHS muddies the water. It seems to primarily base its argument for common law privacy protection on

44. *See* Mont. Const. Conven. Transcripts 632 (1972).
45. MONT. CONST. Art. II, § 10 (emphasis added).
46. 429 U.S. 589 (1977).
47. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 60008.

the Federal Constitutional right to privacy in the accumulation and distribution of IIHI.[48] This position is untenable in that it would only support expenses for prevention of government invasion of individual privacy, a protection that SPIIHI does not even provide except in the narrow circumstance when a state or federal government is functioning as a covered entity.[49]

II. The Existing Problem of Medical Record Privacy

From the very beginning, HHS' approach raises serious questions as to clarity of its ultimate purpose and the chosen path to achieve it. To be effective, it is critical to make informed triage decisions about what information is most important to safeguard and from whom and in what context it must be protected. Unfortunately, SPIIHI fails to adequately address these considerations.

A. The Increasing Potential for Misusing Health Information

The United States healthcare industry is made up of in excess of twelve million providers, suppliers, researchers and payers, in more than 500,000 companies,[50] delivering care through an estimated 2 billion patient encounters per year.[51] The unrestricted rapid flow of medical information is essential to maintaining the best health care system in the world, especially ministering to a mobile population with high expectations.

As technologic sophistication in the gathering, storage, transmission and disclosure of data have advanced over the past three decades, there is little doubt that individual privacy is increasingly jeopardized. The zone of privacy expectation has been gradually, but consistently eroded. If an individual releases data about himself, legal precedent holds that he cannot reasonably expect it will remain private. At the same time, how-

48. *See id.* at 60008-10.

49. *See infra* Part IV for a more detailed discussion of covered entities and when HIPAA and SPIIHI apply to governmental actions.

50. Robert E. Nolan Company, Inc., *Cost and Impact Analysis: Common Components of Confidentiality Legislation* 2 (Fall 1999), <http://www.renolan.com/healthcare/privacy.htm>.

51. *See id.* at Exhibit B. This exhibit uses data publicly available from the Department of Health and Human Services, Center for Disease Control, National Health Interview Survey, American Hospital Association, Health Insurance Association of America, National Center for Health Statistics, National Home and Hospice Care Survey and others to estimate the number of patient encounters per year.

ever, most modern day interactions require some degree of disclosure.

Data collection in and of itself, however, is not the threat. To threaten privacy, data must be converted to useful information that can be further transformed into knowledge compelling action. Scientists and researchers realized long ago that mere large amounts of raw data are relatively inadequate without an algorithm for analysis. The discipline of packaging raw consumer data in such a way it becomes useful information is the science of informatics. The needs and motives of the end user define what is useful. Thus in informatics, data must be packaged differently for a business user than for a consumer, a hospital or a government.

Thus, while there has always been a potential for misuse of IIHI that possibility is clearly embellished by electronic storage and transmission of such data. However, as in most personal issues, it is impractical for the federal government to prevent all potential harms. Instead it should focus on harms that actually exist or are very likely to occur.

B. What Harms Have Actually Occurred?

The question as to what harms actually occurred is a difficult question to answer. HHS and most legislators have chosen to address the question by quoting surveys and describing anecdotes rather than objectively analyzing damages that can be documented. Legislative anecdotes abound and include horrifying cases such as a health worker sending the names of four thousand HIV positive patients to a Florida newspaper and a National Enquirer article about singer Tammy Wynette's supposed liver disease based on purloined medical information.[52] Surveys are also plentiful. SPIIHI's introductory section uses non-scientific survey results on the need for privacy standards to justify its scope stating:

> Indeed, a Wall Street Journal/ABC poll on September 16, 1999, asked Americans what concerned them most in the coming century. "Loss of personal privacy" was the first or second concern of 29 percent of respondents. All other issues, such as

52. *See* Patrick Leahy, Introductory remarks on Medical Information Privacy and Security Act, 143 Cong. Rec. §§ 11689-11691 (daily ed. Nov. 4, 1997).

terrorism, world war, and global warming had scores of 23 percent or less.[53]

These concerns are amplified by other, even more poignant surveys. For example, a recent national survey found over 50% of Americans felt that computer records will make their health care information less secure.[54] Fifty-five percent are concerned that computer hackers will steal their information and 66% are concerned that government and private health insurers will misuse their information.[55] Twenty percent believe that their personal information has already been misused.[56] These numbers are disturbing but, in reality, based only on subjective opinion and may depend significantly on the tone and wording of the survey questions.

More disturbing than the numbers quoted above but still subject to validity criticisms are the statistics from the same survey that seven percent of Americans feel that they have been personally harmed or embarrassed by improper disclosure of their health information.[57] However there is no clear definition of "harmed," no quantification of the extent of the harm and no questioning of whether embarrassment merits federal protection. Fifteen percent claim that they have personally taken steps to protect sensitive information such as changing physicians, paying out of pocket for covered expenses, giving inaccurate information to their physician or avoiding care altogether.[58] However, no objective data confirm these numbers.

Another approach to assess actual harm is to examine court cases in which individuals have felt sufficiently damaged to sue. A Westlaw search for court cases about medical privacy violations between 1990 and the present revealed fewer than 200 hits.[59] Interestingly, however, the majority of those cases were suits against governmental entities that are specifically excluded

53. Standards for Privacy of Individually Identifiable Health Information; 64 Fed. Reg. at 59919.

54. California Healthcare Foundation, *Americans Worry About the Privacy of Their Computerized Medical Records* (Jan. 1999) <http://www.chcf.org/press/viewpress.cfm?itemID=362>.

55. *See id.*

56. *See id.*

57. *See id.*

58. *See id.*

59. Westlaw search on the ALLCASES database using the terms: (MEDICAL) / P (INFORMATION OR RECORD!) /P ("RIGHT OF PRIVACY" OR "RIGHT TO PRIVACY" OR PRIVA!) /P (VIOLATION) & DA(AFT Jan 1, 1990) performed 3/14/00.

by SPIIHI. Unfortunately, this method of estimating damages also has its limits in that it only captures reported cases.

Currently, there is no reliable definition of the actual extent to which medical information privacy has been violated. The potential certainly exists but is that potential really a serious problem? Before embarking on a course that radically alters how medical information is handled by all providers, insurers and other entities covered by SPIIHI.[60] HHS should have undertaken a formal study to determine the actual extent of the problem so that it could properly triage limited resources to the most effective solutions.

C. *Who is Likely to Misuse Health Information?*

An alternative approach to protecting medical record privacy would be to determine which entities are most likely to misuse that information and tailor protection efforts accordingly. SPIIHI ignores this approach altogether and instead tries to extend its regulatory power to reach all possible threats, not only entities specifically covered by HIPAA but extending that reach through contractual arrangements to reach the business partners of those entities.[61] SPIIHI also burdens patients with the difficult and possibly illusory task of negotiating how much of their privacy they are willing to relinquish.

Whether one prefers to quote Willie Sutton's famous explanation about robbing banks "because that is where the money is" or Woodward's Watergate observation about "following the money," both highlight the logic of focusing IIHI protection efforts on instances where IIHI can be used to substantially profit commercial entities. (Other privacy infractions are likely not worth the cost of implementation and enforcement of Federal regulations and are probably dealt with more effectively at a local level.) Doing so, in effect, reduces the field to three major categories of organizations that can process information on a sufficient scale to make it profitable: the three major credit bureaus, insurance companies (through the Medical Information Bureau), and governments.[62] Interestingly, all three of these

60. *See infra* Part IV(D)(3) (financial impact of SPIIHI); *see also* discussion *infra* Part V (B) (closed pool of health care dollars).

61. *See infra* Part IV(B)(3) (covered entities and business partners).

62. The three major credit bureaus which collectively claim to issue four billion credit reports per year and their contact numbers are Equifax at (800) 685-1111, Experian at (800) 682-7654, and Trans Union at (800) 888-4213.

entities have a history of abusing private information for institutional goals.

This necessity for economy of scale required to realize profits is important because it provides the impetus to invade privacy on a scale that is larger than the current privacy laws can address. The three major credit bureaus maintain more than 400 million records in order to generate the necessary scale to profit from that information.[63] Insurance companies did not find individual corporate data collection sufficient to provide profitable information so they united to form the Medical Information Bureau.[64] In contrast, the offices of physicians and other providers and hospitals are not likely to make substantial profits by misusing their patient's private information. The scale is too small to allow sufficient profits to justify the risk of detection and loss of patient confidence. Thus these entities should probably not be included in SPIIHI at all.

III. Federal Privacy Legislation: HIPAA and Beyond

No "right" of privacy for health information is specifically defined by HIPAA.[65] HIPAA mentions the term privacy nine times but never as a right. Rather, it consistently discusses the "need" for privacy of certain health information. On the other hand, the proposed rules begin with the premise that "privacy is a fundamental right"[66] and infer that cost should be a secondary

63. *See* DeCew, *supra* note 8, at 146.

64. MIB was founded in 1938. Based out of Boston, it is an organization with approximately 750 member insurance companies. It collects and furnishes information on consumers to all MIB members for use in the insurance underwriting process. In addition to an individual's credit history, data collected by MIB may include medical conditions, driving records, criminal activity, and participation in hazardous sports, among other facts. MIB's member companies account for 99 percent of the individual life insurance policies and 80 percent of all health and disability policies issued in the United States and Canada. The MIB does not have a file on everyone. Approximately 15 million Americans and Canadians are on file in the MIB's computers. If you think your medical information is on file, you may want to be sure it is correct. You can obtain a copy ($8.50) by writing to: Medical Information Bureau, P.O. Box 105, Essex Station, Boston, MA 02112, or call (617) 426-3660. For more information, you may visit the following web sites: <http://bullybusters.org/home/twd/bb/legal/mib.html> and <http://www.mib.com>.

65. *See generally* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

66. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59918, 60008 (1999) (to be codified at 45 C.F.R. pts. 160-164) (proposed Sept. 11, 1999).

consideration to these rules which "promote the view that privacy protection is an important personal right."[67]

A. HIPAA in General

The primary purpose of HIPAA is stated in the Act itself which provides that HIPAA is intended as:

> [a]n act . . . to improve portability and continuity of health insurance coverage in group and individual markets, to combat waste, fraud and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long term care services and coverage, to simplify the administration of health insurance, and for other purposes.[68]

Nowhere does the purpose statement specifically mention a primary intention to guarantee the security of individually identifiable health information (IIHI) nor can that purpose be implied from any of the explicitly stated purposes. The intent to protect that information falls into the catch-all category of "other purposes." The purpose statement does, however, explicitly mention the intent to simplify and thus, by implication, reduce the cost of health care insurance administration. This is an important observation which will be amplified in the subsequent sections but deserves reemphasis here: HIPAA's primary purpose is at least arguably related to cost and efficiency whereas its mandate to protect privacy is mentioned only secondarily under the umbrella of "other purposes."

However, in fairness, HIPAA is an extraordinarily broad law touching many different areas of healthcare. In addition to its own provisions, HIPAA amended the Employee Retirement Security Act of 1974, (ERISA),[69] the Public Health Service Act, (PHS),[70] and the Internal Revenue Code.[71]

HIPAA is divided into five separate sections with little tying them together. These include: Title I, addressing healthcare access, portability and renewability; Title II, dealing with healthcare fraud; Title III, creating medical savings accounts and speaking to long term medical care, consumer protection and

67. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 60007.

68. Pub. L. No. 104-191, 110 Stat. 1936 (1996) (emphasis added).

69. *See generally* 29 U.S.C. §§ 1001-1461 (1994); *see, e.g.,* 29 U.S.C. § 1181 (1994).

70. *See generally* 42 U.S.C. §§ 201-299 (1994); *see, e.g.,* 42 USC § 300gg-41 (1994).

71. *See generally* 26 U.S.C. §§ 1-9833 (1997). *See* Katherine Benesch, *Healthcare Fraud Criminalization Growing*, 7 N.J. LAW. 1422 (1998).

organ transplantation efforts; Title IV, regulating private group health insurance plans; and Title V, amending the Tax Code in the area of revenue offsets.[72] Overall, HIPAA encompasses more than one hundred fifty single spaced typewritten pages.[73] Buried deeply within Title II (the division on fraud and abuse) rather than in Title III (the division on consumer protection), accounting for less than a single page of the one hundred fifty page document, is Section 264 entitled "Recommendations With Respect to Privacy of Certain Health Information."[74]

Section 264 of HIPAA, is intimately related to Section 262 entitled "Administrative Simplification."[75] Section 262 mandates administrative simplification intended to facilitate processing health care payments by promoting standard formats for electronic information exchange.[76] The drafters of HIPAA realized that standardization of database configurations and the increased use of electronic technology would further decrease the already tenuous security of IIHI. Fearing that the public would not continue to accept the fact that their health information had less protection than their financial data, almost as an afterthought, Congress included a provision to stimulate development of electronic safeguards for health information, HIPAA section 264.

Section 264 of HIPAA is a short, concise statement of Congressional intent to protect the privacy of certain IIHI transmitted in electronic data exchanges.[77] It required HHS to submit to the Senate Committees of Labor and of Human Resources and Finance and the House Committee on Ways and Means detailed recommendations on standards with respect to the privacy of individually identifiable health information by August 1997.[78] It further required those recommendations address three distinct subjects:

(1) The rights that an individual who is a subject of individually identifiable health information should have.

72. *See generally* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

73. The page numbers used for HIPAA in this article were generated by downloading the referenced documents from Westlaw and printing them in a single-spaced 12 point font format on 12/1/99.

74. *See id.* § 264, 110 Stat. at 2033.

75. *See id.* § 262, 110 Stat. at 2021.

76. *See* Alexander Brittin *et al., Understanding HHS's Proposed Health Information Privacy Standard*, 8 BNA HEALTH LAW REP. 1949, 1950 (1999).

77. *See generally* HIPAA, § 264.

78. *See id.* § 264 (a).

(2) The procedures that should be established for the exercise of such rights.
(3) The uses and disclosures of such information that should be authorized or required.[79]

HHS delivered these recommendations to Congress on September 11, 1997.[80] However, between September 11, 1997 and August 21, 1999 Congress failed to reach sufficient consensus to pass legislation governing the privacy of IIHI transmitted in connection with transactions defined in the Social Security Act.[81] This is not to say that Congress did not make an effort; multiple bills and resolutions were submitted each year by members of both political parties, but none made it out of committee.[82]

Congress' failure to enact legislation protecting IIHI by August 21, 1999, triggered part (c) of HIPAA section 264.[83] This section provided that HHS must promulgate final regulations concerning such standards by February 2000. These regulations were clearly intended to be a floor of minimum protection and explicitly would not preempt more stringent state laws.[84]

Arguably the purpose of such regulations was not to give HHS legislative authority but rather to be an interim measure until Congress could pass the necessary, more stringent legislation. It is important also to note that the particular transactions subject to HIPAA mandates are not expansive. They are limited to explicit financial and administrative transactions defined by the statute[85] or transactions deemed by the Secretary of HHS to be consistent with the two precise, limited objectives: specifically the "goals of improving the operation of the health care system and reducing administrative costs."[86]

---

79. *Id.* § 264 (b).

80. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59918, 59920 (1999) (proposed). Full text of recommendations available at <http//aspe.hhs.gov/adminsimp/pvcrec.htm> (visited Feb. 22, 2000).

81. *See* 42 U.S.C. § 1320d-2 (1994).

82. *See, e.g.,* The Fair Health Information Practices Act of 1997, H.R. 52, 105th Cong. (1997); Medical Information Privacy and Security Act, S. 1368, 105th Cong. (1997); The Medical Records Confidentiality Act, S. 1360, 104th Cong. (1995); and Medical Information Protection Act, S. 881 106th Cong. (1999).

83. *See generally* 42 U.S.C. § 1320 (d)(2)(c) (date).

84. *See id.* § 1320 (d)(2)(c)(2).

85. The statute specifically defines the covered transactions as health claims or equivalent encounter information and attachments, enrollment and disenrollment information, eligibility and payment information, health status claims, and referral certification and authorization. *See id.* § 1320 (d)(2)(a)(1 and 2).

86. *Id.* § 1320(d)(2)(a)(1)(B) (emphasis added).

These points prompt a second important observation: the plain language of both HIPAA section 264 and the Social Security Act section 1173(a) limits the scope and purpose of HHS's mandate. In the absence of formal legislation, HHS is only authorized to the promulgate regulations to "adopt standards"[87] on a limited number and type of transactions. Those actions are restricted to measures that both improve the operation of the health care system AND reduce administrative costs. The mandate is clearly not to reorganize the entire information system employed by the healthcare industry. A reorganization of that magnitude requires careful balancing of political interests which only a legislative body can accomplish. This premise will be amplified in subsequent sections of this paper.

IV. Proposed Rule for Standards for Privacy of Individually Identifiable Health Information (SPIIHI)

HHS promulgated SPIIHI on November 3, 1999.[88] On January 5, 2000, HHS issued several corrections to the proposed rule.[89] Taken as a whole, SPIIHI represents a radical deviation from the traditional oversight of medical care. Although in the past HHS has regulated the care it underwrites, personal injury related to medical care has traditionally been adjudicated at a state level using the authority of the states to protect the general welfare of their population. SPIIHI represents the first attempt by the federal government to invade the traditionally state regulated protection from medical privacy violations.[90]

In promulgating its proposed rule for privacy standards, HHS generated more than six hundred pages of complex proposed regulation and explanation.[91] HHS divided SPIIHI into ten subdivisions: (1) background; (2) provisions; (3) small business assistance; (4) impact analysis; (5) flexibility analysis; (6) unfunded mandates; (7) environmental impact; (8) collection of information requirements; (9) federalism; and (10) coordination with Indian Tribal Governments. This section will briefly discuss each of these subdivisions focusing primarily on the two most important subdivisions: provisions and impact analysis.

87. *Id.* § 1320(d)(2)(a)(1).
88. *See generally* 64 Fed. Reg. 59918 - 60065 (1999).
89. *See generally* 65 Fed. Reg. 427-429 (2000).
90. *See* Cassie M. Chew & Mark Felsenthal, *Clinton Releases Proposed Regulation, Officials Stress Limits on HHS' Authority*, 8 BNA Health Law. 1747 (1999).
91. *See id.*

A. Background

SPIIHI begins with a mission statement defining the pressing need for medical privacy standards as rooted in concerns of the American citizenry. To support that position it quotes a Wall Street Journal Poll that identified concern over personal privacy as the number one public concern in front of terrorism, world war and global warming.[92] The section makes the observation that States have variably protected this particular interest.[93] It then invokes the Congressional intent and power of the federal government to intervene by quoting section 264 of HIPAA and defining the problem as national in scope[94] due to the increase in electronic communication of IIPI and interstate transmission of data.[95] Finally, HHS validates its own authority to promulgate these rules based on HIPAA section 264.[96]

A major concern in this background subdivision is HHS' attitude toward cost. As other commentators have observed, the emphasis of SPIIHI is primarily on creating the most comprehensive and effective privacy regulations possible.[97] Therefore in this sweeping reform, cost concerns are minimized. This minimalist attitude toward cost is exemplified in the "administrative cost" paragraph of the background subdivision which states. Thus, even if the rules proposed below were to impose net costs . . . they would still be "consistent with" the objective of reducing administrative costs for the health care system as a whole.[98]

B. Provisions

This subsection is the body of the proposed rule. It is further divided into eleven parts. Because this subsection focuses on the actual application of the rule, it is one of the two most important subsections of SPIIHI and so this paper will briefly address each of those parts individually.

92. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 59919.

93. *See id.* at 59920 (quoting a survey by the Institute for Healthcare Policy and Research).

94. *See* Standards for Privacy of Individually Identifiable Health Information; 64 Fed. Reg. at 59919-59921.

95. *See id.* at 59920.

96. *See id.* at 59921.

97. *See* Institute for Healthcare Policy and Research, *supra* note 93, at i.

98. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 59922.

1. Applicability

This part defines what entities are included and what information is covered.[99] The proposed regulation covers three very broad groups of entities: (1) all health plans (essentially all private or government individual or group insurers including the Federal Employees Health Benefit Plan ("FEHBP") which is excluded from many federal mandates including the HIPAA fraud provisions);[100] (2) all health care clearinghouses (basically any public or private entity which maintains healthcare information including community health information systems, data registries such as tumor or trauma registries, and billing services); and (3) all health care providers. It applies to any individually identifiable health information which has been transmitted electronically no matter what form it takes after transmission (oral or written) which it then defines as "protected health information" (PHI).[101] Basically, once IIHI is transmitted electronically it becomes PHI under the rule.

At first glance, this definition seems to have the potential to miss many healthcare providers who do not routinely use electronic medical records, particularly since the vast majority of health records in this country are still paper. However, when any individually identifiable part of any health record is transmitted electronically, even on behalf of a provider by a billing agent, the transmitted information becomes protected. HHS acknowledges that it is nearly impossible to separate the protected from the non-protected information within a single record. HHS suggests the solution to this is to treat all mixed medical records as protected. The reality of medical practice is that almost all medical records are destined to become "mixed medical records" thus forcing covered entities to apply the standards to all parts of all medical records.

99. *See id.* at 59927-28.

100. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 204 (1996) (referencing 42 U.S.C. § 1320 a-7 (f) which defines Federal Health Plan as "any plan or program that provides health benefits, whether directly, through insurance, or otherwise, which is funded directly, in whole or in part, by the United States Government (other than the health insurance program under chapter 89 of Title 5)" specifically excepting the FEHBP from coverage).

101. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 59937.

2. Definitions

The definition part of SPIIHI, nearly twenty pages long,[102] generally reinforces HHS' purpose of casting as wide a net as possible when protecting IIHI, as illustrated above. One particularly difficult conundrum is identifying the mechanism to de-identify health data. De-identified IIHI is defined as information that has been stripped of the potential to be linked to a specific individual.[103] The rules create a safe harbor of sorts for data which will be classified as "de-identified," but that safe harbor creates only a rebuttable presumption of sufficient de-identification which could be overcome in a civil or criminal action and thus may induce a flurry of litigation.

3. General Rules

The purpose statement at the beginning of the general rules part again reflects the Secretary's broad purpose to regulate all IIHI.[104] It does recognize the necessity to balance the interests of making access to IIHI easy for healthcare purposes and difficult for other purposes but places the onus to achieve that balance on covered entities.[105]

The default position of the rules is to assume that IIHI should not be disclosed without a patient's specific permission subject to a limited number of exceptions based on public policy.[106] The four major exceptions are treatment, payment for that treatment, necessary healthcare operations and a catchall category of "specified public and public policy-related" purposes.[107] HHS specifies that covered entities of all sizes and types will be subject to the same rules, acknowledging but not substantially addressing the problems associated with applying a blanket set of regulations on organizations varying in size and shape by four to five orders of magnitude.[108]

This part then specifies general rules for the use and disclosure of IIHI for treatment, payment and health care operations and includes a special exception for psychotherapy notes. It also

102. *See* SPIIHI, supra at note 29.
103. *See id.* at 59935.
104. *See id.* at 59939.
105. *See id.*
106. *See id.*
107. *Id.*
108. *See id.* (applying the rules equally to all providers, regardless of size, from rural physician offices consisting of a single provider to the largest covered entity that may involve tens of thousands of employees).

addresses research information in great detail. This part also establishes the concept of "Minimum Necessary Use and Disclosure."[109] This concept requires the individual evaluation of every request for IIHI to determine the minimum quantum of information needed to fulfill that request.

In the service of a somewhat murky purpose, the general rules establish the right of individuals to create special or specific restrictions on the use of their IIHI.[110] However, it also gives a covered entity the right to refuse that request and creates a blanket exception to the restriction for governmental entities and public health purposes by referencing proposed §164.510.[111] HHS then acknowledges that the "right" may be difficult to vindicate because most entities will simply refuse to honor such requests due to cost considerations.

In the struggle to reach entities not covered by HIPAA legislation, the general rule holds covered entities liable for violations perpetrated by their business associates.[112] In doing this, the Secretary goes so far as to enunciate specifications for the contracts between covered entities and their business partners.[113]

HHS also holds covered entities liable for the information practices they agree to and publish under the notice requirements of §164.512, which include both posting of a notice and delivery of a notice to the patient.[114]

Finally, the general rules also outline in detail the process by which IIHI can be "de-identified," limit the scope of protection to two years after an individual's death and define how the rule is applied to sub-parts of uncovered entities that conduct health care activities such as school or employer clinics.[115]

4. Uses and Disclosures with Individual Authorization

This part addresses the requirements when PHI is disclosed pursuant to an individual's explicit authorization. HHS reiterates the default position that no PHI can be disclosed without authorization by the individual or law and its intention that

109. *See id.* at 59943-45.
110. *See id.* at 60056.
111. *See id.*
112. *See id.* at 59947-50.
113. *See id.* at 59948.
114. *See id.* at 60059 (to be codified at 45 C.F.R. § 164.512); *see also id.* at 60049 (model notice at Appendix A).
115. *See id.* at 59946, 59950.

these rules not "interfere with normal uses and disclosures" of PHI in the delivery of and payment for health care.[116]

HHS divides explicit authorization into two general groups: disclosure requested by the patient and disclosure requested by the covered entity.[117] It rationalizes this approach by hypothesizing that when individuals initiate authorizations they are more likely to understand the purpose of the disclosure and to intend self benefit.[118] In the case of patient requested disclosure, no limits are placed on disclosure other than a description of the requested information and the disclosing and receiving entities.[119] No statement of purpose is required.[120] Under SPIIHI, the covered entity seems to have the responsibility to assess the request and determine if the individual has "a clear understanding of what information is to be disclosed under the circumstances" although HHS states it would not be "feasible to ask covered entities to make judgments about intended uses."[121] At times it may be difficult to determine if the individual has a clear understanding of the information she is divulging if the purpose of that disclosure is unknown.

The requirements when a covered entity requests disclosure of PHI are more rigorous and are intended to prevent coercion of the individual by the entity.[122] In this case, the disclosure form must at a minimum identify the purpose of the disclosure and the proposed uses of the information and specifically forbids blanket authorizations.[123] HHS clearly intends that the level of patient understanding required for disclosure parallels the medical standard of informed consent with the duty flowing from the covered entity to the individual.[124] The covered entity

116. *Id.* at 59951 (emphasis added) (Although this part does not specifically define normal presumably it includes all situations where explicit disclosure is not required including law enforcement and other governmental needs).

117. *See id.*

118. *See id.* This level of sophistication from patients in healthy situations may be fallacious, let alone in the throes of disease. Is it really likely that the average patient actually knows how her information will be used by a life insurance company, employer or in tort litigation? In the latter case the patient is shifting the information to a non-covered entity with no more reason to trust that person than they have to trust their health care provider.

119. *See id.* at 59952.

120. *See id.*

121. *Id.*

122. *See id.* at 59953.

123. *See id.* at 60055-56 (to be codified at 45 C.F.R. § 164.508).

124. *See id.* at 59953.

has the explicit duty to disclose any financial interest in the authorization.[125]

SPIIHI imposes a plain language requirement on all authorizations, prohibits the conditioning of treatment or payment on disclosure of information not directly related to that treatment or payment, and provides example disclosure forms.[126] It also requires covered entities to keep track of all disclosures, provide the patient a record of those disclosures on demand, maintain a process by which an individual can revoke an authorization and defines expired, deficient or false authorizations as no authorization at all.[127]

5. Uses and Disclosures without Individual Authorization

The SPIIHI preamble extensively elaborates on the rationale behind all uses and disclosures not requiring individual authorization. The principle underlying all of these uses is to "promote key national health care priorities, and to ensure that the health care system operates smoothly."[128] The Secretary states that she considered only allowing such disclosures when affirmatively mandated by law but rejected this notion because the excepted activities are so important to the population as a whole.[129] The following paragraph contains an admission that once this protected information is in the hands of many government entities, it is no longer regulated by the act.[130] Taken together these statements expose the presupposition that the government and its agencies will always act in the best interest of a patient; however, in reality that interest may be eclipsed when the IIHI is perceived critical to public health.

Generally, SPIIHI liberally permits disclosure of IIHI for "public health activities authorized by law" stating explicitly the intention to interpret the phrase broadly.[131] Presumably this intention includes the interpretation of state and local law as well as federal law which undermines the stated major purposes of setting a uniform national floor of protection.

125. *See id.* at 60056 (to be codified at 45 C.F.R. § 164.508 (d) (iv)).
126. *See id.* at 59954.
127. *See id.*
128. *Id.* at 59955 (e.g., permitting the Center for Disease Control to gather and process information and allowing physicians to communicate freely among themselves regarding patient care).
129. *Id.*
130. *Id.*
131. *Id.* at 59955.

SPIIHI also proposes to allow liberal disclosure to public and officially designated private health oversight agencies especially, for the purposes of combating fraud,[132] ensuring non-discrimination and improving quality of care.[133] SPIIHI permits disclosure to the courts and administrative agencies for use in proceedings whenever the information relates to a party of the proceeding or is ordered by a court or administrative tribunal and does not require the protection of a formal judicial subpoena.[134] Law enforcement is similarly entitled to wide unauthorized disclosure pursuant only to administrative process, civil investigative demand or perhaps even only a reasonable suspicion standard.[135] Again, states may vary widely in the amount of medical information they permit law enforcement to access pursuant to the state's police powers thus also undermining SPIIHI's purpose of setting a national floor of protection.

The rules permit a blanket exclusion to use IIHI for "research purposes" regardless of funding source or sources.[136] This exclusion is subject to the protections of an institutional review board or a privacy board as defined in the rules.[137] Research is defined broadly as "a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge.[138] "Generalizable knowledge" is knowledge related to health that can be applied to populations outside of the population served by the covered entity."[139]

HHS depends on the institutional review or privacy boards to balance the privacy interests of the individuals whose privacy is

132. Coincidentally, the United States Department of Justice has declared health care fraud the nation's number one white collar crime priority. *See* Kevin J. Darkin, *Understanding the New Health Care Fraud Legislation*, 12 CRIM. JUST. 30 (1997).

133. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59956.

134. *See id.* at 60067 (to be codified at 45 C.F.R. § 164.510 (d)).

135. *See id.* at 59960-64 (interestingly one justification for this stance is that law enforcement may urgently need medical information when pursuing a fleeing armed suspect–a justification that frankly eludes the creative imagination of this author especially in light of the fact that the information can only be released if the records sought are relevant and material to the inquiry, the request is as specific and narrow as practicable, and deidentified information could not be reasonably substituted; a three part test that may require quite a bit of creative thought during hot pursuit).

136. *See generally id.* at 59967-59971, 60053 (to be codified at 45 C.F.R. § 164.510 (j)).

137. *See generally id.*

138. *See id.* at 59967.

139. *See id.* at 59967-71, 60053 (to be codified at 45 C.F.R. § 164.504).

invaded against the greater benefit of the research to society.[140] Using these definitions and restrictions as the rules are currently written, a large insurance company could assemble a "privacy board" with a single member from an outside entity and approve cleverly written "research protocols" fulfilling the technical requirements of the rule but producing results which never intended to benefit the consumer.[141] Additionally, since there are no requirements to report non-federally funded research projects to a central agency, discovery of an unscrupulous practice would be primarily complaint driven. Such a protocol could be easily hidden in a maze of private corporate business practices.

SPIIHI also permits liberal unauthorized disclosure to medical examiners,[142] state or federal governmental data systems for use in support of policy development, regulation or management,[143] in emergency situations (defined specifically as a situation in which there is imminent threat to the health or safety of any person or the public),[144] to the military for active duty service members,[145] to the Department of Veteran Affairs,[146] to the intelligence community[147] and to the State Department.[148] It permits more limited disclosures for use in hospital directories requiring permission from patients with capacity and assuming permission from patients without capacity.[149] It also permits disclosure to next of kin (or other family member or close personal friend),[150] for use in banking and payment processes,[151] and other uses "as required by law."[152]

---

140. *See id.* at 60058.

141. *See id.* at 60058 (to be codified at 45 C.F.R. § 164.510 (j)).

142. *See id.* at 59960.

143. *See id.* at 59964.

144. *See id.* at 60058 (to be codified at 45 C.F.R. § 164.510 (k)).

145. *See id.* (to be codified at 45 C.F.R. § 164.510 (m)).

146. *See id.*

147. *See id.*

148. *See id.*

149. *See id.* at 59965-66.

150. *See id.* at 60058 (to be codified at 45 C.F.R. § 164.510 (l)). It is hard to understand the need for this provision that defers to local applicable law and ethics to codify an already existing responsibility which varies greatly from state to state. It is further mystery that next of kin is carefully defined but close personal friend is not and requires no identity check to confirm.

151. *See id.* at 59966-67.

152. *Id.* at 60059 (to be codified at 45 C.F.R. § 164.510 (m)).

6. Rights of Individuals

SPIIHI is specifically intended to create what HHS describes as "four basic individual rights:" (1) the right to written notice of information practices; (2) the right of an individual to obtain access to her own IIHI; (3) the right to an accounting of how an individual's IIHI has been disclosed; and (4) the right to request amendment and correction of PHI.[153] SPIIHI strictly regulates the exact quantum of notice to which an individual has a right. This right to notice includes a "plain language" mandate, an explicit statement of all four rights and how to vindicate them, and a statement of required components of the notice.[154]

7. Administrative Requirements

This part is intended to compel covered entities to establish certain safeguards for PHI including designating a privacy official, training the members of their workforce about privacy requirements, and establishing sanctions for members of an entity's workforce who violate the policies and procedures.[155] It also establishes a duty to mitigate the harm caused by any inadvertent disclosure of PHI.[156]

8. Development and Documentation of Policies and Procedures

This part of SPIIHI instructs covered entities to develop and document written policies and procedures for implementing the requirements of this rule.[157] In essence, even the smallest solo practitioner's office would be required to have a policy and procedures manual and to store the records of all transactions covered by this rule for a minimum of six years. HHS emphasizes that the scale of the written policies should match the size of the institution.[158] Those policies would include how PHI is used and disclosed, how requests for restricting uses and disclosures are

153. *See id.* at 59976-88, 60059-62 (to be codified at 45 C.F.R. §§ 164.512, 164.514, 164.515, 164.516).

154. *See id.*

155. *See generally id.* at 59988-91, 60061-62 (to be codified at 45 C.F.R. § 164.518).

156. *See id.* at 60062 (1999) (to be codified at 45 C.F.R. § 164.518(f)).

157. *See generally id.* at 59991-94, 60062-63 (to be codified at 45 C.F.R. § 164.520).

158. *See id.* at 59992. (One suggestion that is made is for smaller institutions to restrict access to a single employee-a completely unworkable solution. In the opinion of this author, this suggestion, while well intended, underscores the lack of knowledge on the part of SPIIHI's drafters about how medical offices function, especially in underserved rural areas.)

honored, how disclosures are tracked, how the administrative requirements are met, how notice of information practices is provided to patients, a policy for patient inspection and copying of records, and a procedure to allow amendment of the records. Covered entities would also be required to keep samples of all relevant forms.

9. Relationship to Other Laws

SPIIHI, reflecting HIPAA's explicit mandate, specifically sets out a general rule that state law provisions contrary to its provisions or requirements are preempted.[159] The rule states that HHS does not intend to preempt all state regulation by occupying the entire field. Rather, the rule is intended only to preempt conflicting laws.[160] The statute provides three exceptions to this general rule: (1) for state laws which address controlled substances; (2) for state laws relating to IIHI that are contrary to and more stringent than the federal requirements; and (3) a catchall category to prioritize state laws which the Secretary of HHS determines are necessary to prevent fraud and abuse, to ensure regulation of insurance and health plans, for state reporting on health care delivery, and for other purposes.[161] HHS clarifies five ambiguities in interpreting HIPAA and the rule including the precise definitions of "provision of," "contrary to," and "state law;" the meaning of "relates to the privacy of IIHI;" and the definition of "more stringent." It then attempts to preempt confusion and avoid potential litigation over these terms by enunciating its own position on their interpretation.[162]

HHS also articulates its official position of how SPIIHI interrelates to existing federal laws.[163] The language of this section takes on an almost judicial quality as it discusses the principles of statutory interpretation behinds its position.[164] This part ends by concluding that SPIIHI does not preempt the Privacy Act,[165] more stringent privacy requirements of the Substance Abuse

159. *See id.* at 59994-99.
160. *See id.* at 59994.
161. *See id.*
162. *See id.* at 59994-99.
163. *See id.* at 59999-60002.
164. *See id.* at 59999-60000.
165. *See* 5 U.S.C. § 552 (a) (1999).

Confidentiality Regulations,[166] or settled ERISA preemption law.[167]

10. Compliance and Enforcement

Though initially the enforcement of compliance with SPIIHI will be largely complaint driven, HHS also anticipates an active program to monitor and review entity compliance.[168] Individual complaints directly to the Secretary will undoubtedly be burdensome but may result in a better clarification of the scope of the problem of privacy violation.[169]

The rules as written stress cooperation to achieve compliance, anticipating HHS would offer technical assistance and guidance.[170] Whether HHS and its investigative division, the Office of the Inspector General (OIG), actually have the human resources to accomplish a task of this magnitude remains to be seen.[171]

Although § 264 of HIPAA does not specifically outline penalties for privacy violations, HHS assumes that §§ 1176 and 1177 will apply to SPIIHI. HHS, without further explanation, assumes that SPIIHI is subject to HIPAA's two-pronged approach to enforcement.[172] It asserts that the Secretary has the authority to impose civil monetary penalties against those covered entities

166. *See* 42 C.F.R. part 2 (1999).

167. *See* 29 U.S.C. § 1001 et. seq. (1999).

168. *See generally* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 60002-03, 60063-64 (to be codified at 45 C.F.R. § 164.522).

169. As is argued in other sections of this paper, perhaps identifying the problem should have been the first step, taken prior to the development of this rule.

170. *See generally* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 60063-64 (to be codified at 45 C.F.R. § 164.522).

171. *See generally* OIG Special Advisory Bulletin on Gain Sharing Arrangements and Civil Monetary Penalties for Hospital Payments to Physicians to Reduce or Limit Services to Beneficiaries, 64 Fed. Reg. 37985 (1999). Unfortunately, it appears that the OIG has the sentiment that when Congress passed HIPAA, it failed to adequately provide for the increased manpower such advisory opinions require. In its SAB, the OIG states that gain-sharing arrangements "pose a high risk of abuse." It opines that such arrangements "will require ongoing oversight both as to quality of care and fraud" and declares that it has "neither the resources nor the expertise to police a multitude of such arrangements on an ongoing basis." *Id.* at 37987. Finally OIG completely throws up its hands calling for legislative rather than administrative resolution of the gain-sharing quagmire stating that "case by case determinations by advisory opinions are an inadequate and inequitable substitute for comprehensive and uniform regulation." OIG itself has strongly implied that it currently lacks the resources to fulfill its existing commitments to individually review potential gain-sharing arrangements.

172. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 60003.

that fail to comply in accordance with HIPAA § 1176.[173] These penalties are to be imposed according to the procedures established for imposition of civil monetary penalties in HIPAA.[174] The penalties are capped at $25,000 per year for each inadvertent violation. Also, SPIIHI asserts that HIPAA § 1177 establishes criminal penalties of up to ten years imprisonment and $250,000 for certain intentional wrongful disclosures of individually identifiable health information.[175]

It is important to underscore the fact that the entire burden for enforcement of this provision falls on HHS. There is no private right of action. Therefore, while SPIIHI may set some minimum standards for privacy that will be useful in establishing a standard of care for tort suits by individuals whose information has been misused, it does not provide any avenue to either streamline, enhance or insure recovery for individuals damaged by a covered entity's failure to comply with these standards.

11. Effective Date

A covered entity must be in compliance not later than 24 months following the effective date of the final rule, except for a small health plan that has 36 months to comply.[176]

C. Small Business Assistance

SPIIHI establishes the first federally required regime of information practices for private medical industry.[177] Recognizing that the complexity of SPIIHI could suggest that the requirements imposed on small businesses (comprising eighty-five percent of the medical industry) may be too costly and burdensome, HHS promulgated this section to assist small businesses with compliance.[178] It states that physicians who disclose patient information only in routine medical business could do so without any change in current practices.[179] While this may be possible in some very small number of cases, most doctors will be required to occasionally give out some IIHI requiring that

173. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 1176, 110 Stat. 1936, 2028 (codified at 42 U.S.C. § 1320d-5).
174. *See id.* (referencing § 1128A).
175. *See id.* § 1177 (codified at 42 U.S.C. § 1320d-6 (1999)).
176. *See generally* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 60064 (to be codified at 45 C.F.R. § 164.524).
177. *See id.* at 60003.
178. *See id.*
179. *See id.*

they at least implement the practices and procedures required by the rule even if they rarely use them. Perhaps a better approach would be to eliminate health care providers from the rule altogether.

The Secretary also states that HHS plans to engage in outreach and education programs to ease the implementation of this rule for small businesses, pledging to work with professional associations[180] to provide the greatest possible guidance to small businesses covered by this rule.[181] This again raises the question of whether has the resources to fulfill its obligations.[182]

As a gesture of its intent to live up to this pledge, HHS devotes approximately three pages of its six hundred page document to setting out fourteen principal (though emphatically not exclusive) requirements. These principal statements are simply more concise reiterations of the guidelines outlined in the document as a whole. This section does not substantively exempt small businesses from any of the rule's burdens.

D. Preliminary Regulatory Impact Analysis

This section of SPIIHI is divided into seven parts: (1) the relationship of the analysis to other HIPAA regulations; (2) a summary of costs and benefits; (3) the need for the proposed action; (4) baseline privacy protections; (5) costs; (6) benefits; and (7) an examination of alternative approaches. These areas can be conveniently grouped under four major headings: an introduction to the problem (parts one and two), rationale for regulation of IIHI (part three), actual impact analysis (parts four, five and six), and alternatives (part seven). This section will discuss each of those four major areas in turn.

180. While this is potentially a place to begin reaching physicians, it is important to remember that only about 40% of licensed physicians belong to the AMA, the largest professional association for small physician small businesses.

181. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 60003.

182. Small providers already complain bitterly that HHS fails to provide them adequate guidance in trying to comply with the fraud and abuse requirements of HIPAA. Personal interview with Joan Ashley, director of the Medicaid Surveillance Utilization Review Service (SURS) in Helena, Montana 4/6/99.

1. Introduction to the Problem

Based on several federal requirements,[183] the SPIIHI preamble sets out a "preliminary impact analysis" concerning the effects of the proposed rule.[184] However, in doing so, HHS goes beyond a dispassionate impact analysis and issues a statement strongly advocating global extensive regulation of IIHI that is more a cost/benefit breakdown than an impact analysis.[185] The Unfunded Mandates Act of 1995 requires a cost/benefit discussion but by interweaving the impact analysis with a discussion of costs compared to benefits, the raw impact of the rule is obscured by an argument highlighting the benefits of the rule.[186]

HHS starts by stating it has three basic objectives in promulgating SPIIHI: (1) to establish baseline standards for health care privacy protection; (2) to establish a uniform base protection for all health information maintained or transmitted by covered entities; (3) protect the privacy of health information maintained in electronic form as well as information generated by electronic systems.[187] It acknowledges the difficulties inherent in measuring the costs of these objectives because there is very little data available on the financial impact of privacy protection.[188] The economic burdens of several elements are simply omitted because HHS could not make realistic estimates.[189] However HHS does acknowledge that the cost of these burdens will be significant.[190] Further, HHS' financial analysis is not based on total costs of its implementation but rather the incremental costs above those attributable to other HIPAA regulations, adding more error into a system in which accuracy is already questionable.[191] HHS also observes benefits are even harder to quantify than costs given the underlying assumption

183. *See* 5 U.S.C. §804 (2) (1999); *see also* Exec. Order No. 12,866, 58 Fed. Reg. 51,735 (1993) (requiring an impact analysis for regulations that exceed certain levels of impact).

184. *See generally* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 60005-36.

185. *See id.* at 60006.

186. *See* Unfunded Mandates Reform Act of 1995, Pub. L. No. 104-4.

187. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 60005.

188. *See id.* at 60006.

189. *See id.*

190. *See id.*

191. *See id.*

that privacy is primarily a "right" and a "commodity" only secondarily.[192]

2. The Need for the Proposed Action

This part is misnamed. It should really be entitled "a justification for the extent of the proposed action." The "need" for a regulation enunciating medical privacy standards is explicit in HIPAA § 264 (c).[193] Further, few would argue with the concept that IIHI merits some type of protection. The more important issue is to what extent and at what cost the federal government should be in the business of protecting IIHI.

HHS' argument for extensive administrative control is based on a statement of the worst case scenario:

> If the medical system shifts to predominantly electronic medical records in the near future, without the use of accompanying privacy rules, then one can imagine a near future where clerical and medical workers all over the country may be able to pull up protected health information about individuals - - without meaningful patient consent and without effective institutional controls against further dissemination.[194]

The argument is reinforced by HHS' position that:

> Privacy is a fundamental right. . . [and] has to be viewed differently than any ordinary economic good. Although the costs and benefits of a regulation need to be considered as a means of identifying and weighing options, it is important not to lose sight of the inherent meaning of privacy: it speaks to our individual and collective freedom.[195]

HHS' clear message is that the privacy of IIHI is in clear and present danger and the urgent duty to protect that information supersedes financial considerations based on the fundamental right to privacy.

HHS develops this argument based on the concept of market asymmetry and the growth of information technology. Patients have less information about how their IIHI will be used and less power to demand protection than the organizations collecting the information.[196] Companies have an incentive to overuse IIHI based on the dollar value of that information both inter-

192. *See id.*

193. *See* Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, § 264 (c), 119 Stat. 2033 (1996).

194. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 60009.

195. *Id.* at 60008.

196. *See id.* at 60008-09.

nally through non-permissive misuse and externally through sale of IIHI to other companies which value it.[197] HHS makes the point that in the current milieu it is expensive and ineffective for a patient to try to personally monitor and control what is done with their IIHI.[198] These difficulties are enhanced by the third party nature of insurance and payment systems which may deny patients the standing to protect their IIHI.[199] Essentially, patients trade financial risk imposed by uncertain healthcare expenses for control over their IIHI.

HHS emphasizes the recent and escalating nature of the problem by noting that with paper records, the risk of information misuse is low because it was expensive and time consuming to access and duplicate medical records but with internet technology, electronic information can be accessed, processed and used immediately and inexpensively.[200] HHS assumes that given the current commercial incentives and barriers to individual patient control, misuse of IIHI will dramatically increase. Lastly HHS makes the point that lack of privacy safeguards may adversely affect health care delivery compromising efficiency through foregone or inappropriate treatment due to patient reluctance to share information with physicians.[201]

Taken in its entirety, HHS has put forth an interesting, but fatally flawed argument for global administrative regulation of all IIHI. The lethal fault is that HHS has failed to adequately prioritize spending. In a political climate where the American legal system has not even yet recognized access to health care[202] as a "fundamental right," HHS argues that the right to protect information generated in the health care delivery process *is* fundamental and justifies major expenditures. While the country struggles to come to grips with the reality that the finite resources available to deliver health care demand cost containment and even rationing, HHS maintains that the cost of protecting IIHI is superseded by the urgent need for absolute confidentiality.

197. *See id.* at 60009.
198. *See id.*
199. *See id.*
200. *See id.*
201. *See id.*
202. Clearly a major sticking point in the concept of a fundamental right to health care is the inability to agree on what the definition of health care encompasses and what subset of that care is implicitly fundamentally due to citizens under the penumbras of the explicit rights.

Prioritizing the spending of health care dollars is the administrative equivalent of medical triage. Within this analogy, HHS mis-triages the value of privacy. It focuses on a relatively minor wound (privacy invasion) in the midst of a life threatening injury (diminishing resources relative to the demand for medical care). In essence, with SPIIHI as written, HHS applies a Band-Aid to a skinned knee while its patient, the American populace, exsanguinates.

3. Impact Analysis

SPIIHI's impact statement is among the most controversial parts of the preamble to the regulation. The controversy arises because the analysis is based on minimal hard data, ignores several major potential costs and varies by an order of magnitude from the only estimate of privacy regulation cost generated in the private sector available, the Nolan Report (commissioned by the Blue Cross/Blue Shield Association).[203] Accordingly, this paper will address HHS' analysis in substantial detail and compare it as closely as possible to the Nolan Report.

a. Establishing a Baseline

HHS starts its impact analysis with a determination of current requirements and practices with regard to IIHI.[204] It states that most current privacy practices stem from existing state laws or professional codes of conduct and ethical behavior, pointing out that states vary dramatically and professional codes do not have the force of law.[205]

Regarding professional codes of conduct, HHS identified three major themes: (1) the need to maintain and protect IIHI; (2) the need for policies to ensure the privacy of IIHI; and (3) the principle that only the minimum needed information should be released.[206] In the proposed regulation, HHS has added to these principles, the right of individual access, the right of notice regarding privacy policies, the requirement to maintain databases of released information, and the mandate to control business partners by contractual agreements.[207]

203. *See generally* Robert E. Nolan Company, *supra* note 50.
204. *See* Standards for Privacy of Individually Identifiable Health Information; 64 Fed. Reg. at 60010.
205. *See id.*
206. *See id.*
207. *See id.* at 60010-11.

In discussing state laws which may be preempted, HHS acknowledges the complexity of the state regulatory system already in effect, citing Florida's more than sixty privacy laws as an example of that complexity.[208] HHS acknowledges its inability to comprehensively study the effects of SPIIHI on state laws and its heavy reliance on the Georgetown University Privacy Project's study on state laws,[209] another admittedly non-exhaustive review.[210] Thus, although HHS has not looked intensively at state laws, it reaches the conclusion that SPIIHI applies some new standards to all states (e.g. requiring covered entities to provide notice of privacy and access policies to patients)[211] and represents a "more level floor from which states could expand privacy protections. . . ."[212]

b. *Overview and Summary of Costs*

Starting from this very sketchy determination of current levels of privacy, HHS proceeds to estimate the costs of the increased levels of privacy protection provided by SPIIHI.[213] HHS points out that covered entities will be implementing these regulations at the same time they are implementing other HIPAA mandated administrative simplification requirements making the incremental increase due solely to SPIIHI difficult to determine.[214] HHS also estimates that the regulations will affect "about 20,000 health plans . . . and hundreds of thousands of providers."[215]

HHS summarizes the cost estimate for implementation of SPIIHI as 1.2 billion dollars for the first year and a five-year total cost of 3.8 billion dollars (with a potential variance of between 1.8-6.3 billion).[216] It then makes comparisons based on its estimate, finding that the cost of SPIIHI represents only 0.1% of the entire healthcare budget for the first year, 1% of the 5 year

208. *See id.* at 60011.

209. *See* Janlori Goldman, *The State of Health Privacy: An Uneven Terrain,* <http://www.healthprivacy.org/resources/statereports/contents.html> (visited Mar. 1, 2000).

210. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 60010.

211. *See id.* at 60013.

212. *Id.*

213. *See id.* at 60014-19.

214. *See id.* at 60014.

215. *See id.*

216. *See id.* at 60006.

increase in healthcare spending[217] and an increased cost of $0.46 per health encounter.[218]

HHS' estimate is an order of magnitude lower than the $43 billion for the first five years published in the Nolan Report.[219] The Nolan Report estimates the effects of the regulation will reach twelve million providers, payers, researchers and suppliers in 500,000 companies, not for profit organizations and research facilities, also an order of magnitude higher than HHS' prediction.[220]

It is important to note that HHS acknowledges that its estimate completely ignores many costs because it found the data too complex to quantify.[221] These omissions include the cost of the minimum necessary disclosure requirement, the outlay to monitor and assume responsibility for business partners, the expense of creating de-identified data and internal complaint processes, the potential cost of the sanctions, compliance and enforcement, the expense to create a privacy board and designate a privacy official, and the additional financial burden of research and optional disclosures.[222] Ignoring such significant potential expenditures raises a serious question about the validity of these numbers; in fact, HHS' estimates may serve as nothing more than an absolute minimum cost the public could expect to incur.

c. Initial Costs

HHS states that "initial costs . . . for the privacy standards should be small" because many of these costs will already be committed for implementation of other HIPAA mandates[223] Although the term initial is not precisely defined, this paper will define initial costs as one time costs for setup and training costs whether they occur in the first year or over five years. As such HHS' categories of Privacy Policies and Procedures, System Compliance Costs, and Training will be considered together. HHS allocates a development cost of $300-$3000 for providers and $300-$15,000 for health plans totaling $395 million over five

217. *See id.* at 60007.
218. *See id.*
219. *See* Robert E. Nolan Company, *supra* note 50.
220. *See id.* at 2.
221. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 60007.
222. *See id.*
223. *See id.* at 60015.

years.[224] HHS has previously estimated that the cost of computer upgrades for all of HIPAA will total $5.8 billion dollars over 5 years.[225] It allocates $90 million to SPIIHI bringing the total to $485 million.[226] HHS also downplays the cost of training personnel, calling it minimal and estimating it at $20/year for provider offices and $60-100/year for health plans and hospitals.[227] This translates to another $110 million over five years bringing initial costs to $595 million.[228]

In contrast to HHS, the Nolan Report estimates initial costs will total $23.4 billion for five years.[229] A strict comparison between the two estimates is not entirely valid because the two reports use somewhat different terminology and assumptions. However, they are similar in that both deal with the costs of implementing the new infrastructure. The Nolan Report includes the costs of the information protection officer based on organization size, salaries and time estimates; the cost of staff training based on lost staff time and cost of the trainer; the cost of computer system changes based on interviews with systems analysts and health care executives using general mission descriptions and costs of reprogramming, testing and coordination with other systems; and the legal costs to review existing contracts for compliance.[230]

d. Inspection, Copying, Amendment and Correction Costs

HHS assigns $2.44 billion in costs over five years for inspection, copying, amendment and correction costs.[231] Interestingly it does not front load any of these costs. Given the level of concern over privacy of IIHI attributed to the public by HHS and Congress, front-loading these costs to take into account an initial rush to vindicate these new "rights" would seem prudent.

HHS estimates the increase in inspection and copying costs to be relatively small because more than half the states already permit this process. However, this ignores its own assumption that notice of the existence of the right will increase awareness

224. *See id.*
225. *See id.*
226. *See id.* at 60017.
227. *See id.*
228. *See id.* at 60015, 60017.
229. *See* Robert E. Nolan Company, *supra* note 50, at 3.
230. *See id.* at 9, 22-26 and Exhibits G, H, I, J.
231. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 60016-17.

and utilization of the right. HHS assumes administrative costs of $10/request and copying costs of $.032 per page based on a study done in 1998 by the Tennessee Comptroller of the Treasury.[232] It acknowledges that other studies have estimated significantly higher costs but chooses this particular study based on the criteria that older studies did not adequately account for savings from computerization.[233] However, this ignores the fact that most records are still paper records and therefore the estimate may be significantly low.

It also does not account for compliance with the new requirement that only the minimum necessary information is released. This fact will increase the level of training required for those record technicians and involve higher level decisions more often, both of which will increase the cost of record copying. HHS' final estimate for inspection and copying over five years is $405 million based on an estimate that only 1.5 percent of patients will request to inspect and copy their records.[234] HHS also asserts that this sum will be paid for entirely by the consumer.[235] This assumption ignores the legal precedent that when a privilege rises to the level of a right, courts often are willing to guarantee it regardless of economic status. When a significant segment of the population is prevented from copying their records for financial reasons, courts may order the inspection, copying and amendment expenses to be borne institutionally or publicly.

In discussing the right to amend and correct the records, HHS does estimate that requests to amend will significantly increase over current demands.[236] However, HHS assumes without explanation or justification that a clerk or nurse can correct most records.[237] It also acknowledges excluding the cost to resolve any disputes arising from disagreements over the contents of records.[238] Using a cost estimate of $75 per record amended and assuming that two thirds of inspection requests will result in amendment requests, HHS estimates that $2 billion will be spent over five years on amendment and correction.[239] When

232. *See id.* at 60016.
233. *See id.*
234. *See id.*
235. *See id.*
236. *See id.* at 60016-17.
237. *See id.*
238. *See id.*
239. *See id.*

added to the $405 million dollars for inspection and copying, the total cost estimated by HHS for inspection, copying, amendment and correction comes to $2.44 billion.[240]

The Nolan Report estimates that inspection, copying and amendment will cost $3.3 billion over five years.[241] It bases this on estimates that 1.25% of hospital patients, 2.0% of ambulatory encounters and 0.5% of health plan patients will ask to inspect and copy their records. It predicts about 35% of those would request amendment and 20% of amendments would go to appeal.[242] It then develops a task list for each process and, based on labor costs and time allocated per task, estimates a per transaction cost.[243]

e. Costs of Written Authorization

HHS estimates the cost of written authorization at $271 million over five years based on the assumption that because authorization is not required for treatment or payment disclosures, authorization will be required in only 1% of all encounters.[244] The Nolan Report on the other hand assumes that most plans will want to collect IIHI data about patients for some reason other than an exempted one (e.g. determinations of health coverage). It again develops a task list for each process and, based on labor costs and time allocated per task, estimates a per transaction cost which translated to $1.9 billion over five years for form creation, legal review, printing, mailing, answering inquiries and new data entry.[245]

f. Costs of Tracking Disclosures

HHS estimates that most of the tracking costs will be subsumed in the $90 million allocated to data system costs discussed above.[246] It predicts ongoing costs would be data entry time alone which it dismisses as de minimis.[247] Thus, nothing is added

240. *See id.*
241. *See* Robert E. Nolan Company, *supra* note 50, at 3, 8, 20-21 and Exhibits E-1, E-2.
242. *See id.*
243. *See id.*
244. Standards for Privacy of Individually Identifiable Health Information, 24 Fed. Reg. at 60017.
245. *See* Robert E. Nolan Company, *supra* note 50, at 3, 6, 13-14 and Exhibits A-1, A-2, and A Support.
246. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 60017.
247. *Id.*

to the bottom line for costs related to tracking. It is simply unlikely that the requirement to track disclosures will add nothing to the costs of SPIIHI.

The Nolan Report, on the other hand, overestimates tracking costs at $9.1 billion over five years.[248] The estimate is inaccurate because it assumes that all disclosures, including those between individual providers for the purposes of referral and between providers and payers for the purpose of payment, need to be tracked ($3.9 billion disclosable encounters).[249] But, SPIIHI stipulates that only a small percentage of disclosures will need to be tracked. Thus the cost of tracking disclosures will likely be less than $9.1 billion. If even one percent of all disclosures are trackable, the five-year cost would be nearly $1 billion using the Nolan Report's methods.

g. Other costs

Another element of SPIIHI that will generate costs is its notice requirement. In this instance, the HHS and Nolan Report estimates are relatively similar with five-year predicted costs of $470 million[250] and $654 million[251] respectively.

HHS estimates that SPIIHI will cost the Federal Government $31 million for the necessary compliance measures associated with privacy protection in its multiple roles as a provider and underwriter of health care, law enforcer, public health record keeper, and health researcher.[252] HHS estimates costs to state governments to be $90 million over five years mostly for expenses generated in a state's role as provider and underwriter of health care. The Nolan Report does not address these costs.

h. Benefits

HHS chooses to discuss potential benefits of SPIIHI in qualitative and quantitative terms. In qualitative terms, it describes these positive effects as "important societal benefits."[253] These include establishment of privacy protection as a fundamental

248. *See* Robert E. Nolan Company, *supra* note 50, at 3, 7, 15-19 and Exhibits B, C-1, C-2, D.

249. *See id.* at 15 and Exhibit B.

250. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 60016.

251. *See* Robert E. Nolan Company, *supra* note 50, at 20.

252. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 60007.

253. *Id.*

right, an increase in the public confidence about the security of their health information, and an increase in the likelihood that "many people" will seek treatment for particular classes of diseases such as mental health conditions, certain cancers, HIV/AIDS, and other sexually transmitted diseases,[254] since sensitive information is federally protected. HHS assumes that this would promote earlier utilization of services and eliminate the added cost of delayed treatments and reduce transmission of communicable diseases.[255] This assumption turns on the idea that large numbers of people currently forego access to medical care based on privacy fears. In reality, the reluctance to seek medical care is more likely due to cost, fear of disease and ignorance. HHS also overlooks the plain fact that every increase in utilization of the system translates into increased health care expenditures.

In quantitative terms, HHS combines its cost estimates with Census Bureau data and arrives at the figure of $3.41 per patient per year additional costs for the benefit of increased IIHI security.[256] Using data on the numbers of health care encounters, HHS arrives at a cost of $0.46 per visit. Using this cost/benefit ratio analysis, SPIIHI may seem quite reasonably priced. However it is important to remember that the Nolan Report suggests that these costs may be higher by a factor of ten and thus the cost/benefit ratio would increase proportionately.

4. Alternative Approaches

HHS goes into considerable detail justifying why it chose this particular set of regulations over other options it considered in its mission to protect the privacy of IIHI. The general approach HHS takes is to assert that provisions could have been more extreme but that it took the more moderate stance.[257] Commentators have suggested this section is merely a preemptive justification aimed at the inevitable challenges.[258] While the section provides some interesting background, these more extreme ap-

254. *See id.* (Making the assumption that medical privacy concerns prevent patients from obtaining early testing and screening for certain types of cancer). This assumption is not supported by information on the ACS website referenced in the next sentence nor any study quoted in the paper. *See id.* at 60019-60022.

255. *See id.* at 60020.

256. *See id.* at 60019.

257. *See* Brittin, *supra* at note 76.

258. *See id.*

proaches which HHS rejected ultimately lend little to an understanding of the rule as it is currently written.

E. Flexibility Analysis

The Regulatory Flexibility Act[259] requires a "flexibility analysis" if a proposed rule would have a significant impact on a substantial number of "small entities" as defined by the Small Business Act.[260] In the health care industry, a small business is defined as a business with less than $5 million in annual revenues, not for profit entities and small government jurisdictions of less than 50,000 citizens.[261] Individuals (sole proprietorships) are not considered small entities.[262] Since the vast majority of hospitals are not for profit and most physicians, even those engaged in solo practices, operate as professional corporations, small entities make up a large majority of health care businesses.[263] Although, estimates of the impact on these small entities varies by an order of magnitude (see impact discussion supra), the rule has a significant impact even using the most conservative estimates.[264] Therefore a flexibility analysis is required.

A flexibility analysis must address six issues: (1) reasons for promulgating the rule; (2) objectives and legal basis of the rule; (3) the number and types of small businesses affected; (4) the specific activities and costs associated with compliance; (5) options considered to minimize the burdens; and (6) other rules that may duplicate, overlap or conflict with the proposed rule.[265] The purpose of a flexibility analysis is to determine if a rule has a differentially large burden on small versus large businesses and ensure that the rule making body has attempted to minimize a disproportionate burden on small businesses. In most cases, larger businesses dominate an industry and therefore a flexibility analysis protects small businesses from unfair bur-

259. *See* 5 U.S.C. § 601 (1999).

260. *See* Pub. L. No. 85-536, 72 Stat. 384 (1958) (codified at 15 U.S.C. §§ 631-657 (1994)).

261. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 60036.

262. *See id.*

263. Using reports form the Small Business Association, HHS estimated that more than a million small health care businesses would be affected, about 84% of the entire health care industry. *See id.* at 60036-38.

264. *See supra* Part IV(D)(3).

265. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 60036.

dens. In the case of health care businesses, small businesses dominate the market and thus the flexibility analysis has less significance apart from the general discussion in the preamble. This paper has already addressed issues 1, 2, 3, and 6 and that discussion will not be repeated. Issues 4 and 5 warrant some brief consideration.

Because the proposed regulation is so onerous, HHS considered excepting small businesses altogether.[266] However, since small businesses make up 84% of the total market, it found this course untenable.[267] HHS also considered extending the time periods for compliance but found this route inappropriate for the same reason.[268] Thus, HHS finally decided that the regulation must apply to covered entities of all types and sizes in order to be effective.[269]

Having decided that it must increase the burden to small entities but also recognizing that most small health care businesses operate close to the margin and are in an environment of massive cutbacks already, HHS advocates the concept of "scalability" in applying SPIIHI. Unfortunately, HHS does not precisely define scalability. It does, however, give some insight into its meaning by stating:

> The privacy standards would need to be implemented by all covered entities, from the smallest provider to the largest, multi-state health plan. For this reason, we propose the privacy principles and standards that covered entities must meet, but leave the detailed policies and procedures for meeting these standards to the discretion of each covered entity. We intend that implementation of these standards be flexible and scalable, to account for nature of each covered entity's business, as well as the covered entity's size and resources. A single approach to implementation of these requirements would be neither economically feasible nor effective in safeguarding health information privacy. Instead, we would require that each covered entity assess its own needs and devise and implement privacy policies appropriate to its size, its information practices, and its business requirements.[270]

266. *See id.* at 60038. .

267. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 60038.

268. *See id.*

269. *See id.*

270. *See* Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, Fed. Reg. 59918, 59925 (1999).

> How each privacy standard would be satisfied would be business decisions that each entity would have to make. This allows the privacy standards to establish a stable baseline, yet remain flexible enough to take advantage of developments and methods for protecting privacy that will evolve over time.[271]

Thus, in the context of this rule, scalability seems to mean that HHS intends to take into account size, purpose and economic status of an entity when enforcing SPIIHI. HHS then gives some examples of how scalability could be applied in entities varying from large insurers to individual provider offices:

> We expect that sanctions would be more formally described and consistently carried out in larger, more sophisticated entities. Smaller, less sophisticated entities would be given more latitude and flexibility. For such smaller entities and less sophisticated entities, we would not expect a prescribed sanctions policy, but would expect that actions be taken if repeated instances of violations occur.[272]

While this plan laudably attempts to minimize burdens on smaller entities, it opens a mine-field of potential litigation over what is fair to expect from entities of varying size, type, and level of sophistication.

Given its policy on scalability, HHS goes on to speculate that absolute costs will then be lower to smaller entities but acknowledges that smaller entities will bear the cost as a larger portion of total revenue.[273] HHS does not address the issue that since smaller entities often have lesser margins of profit, this regulation may have the effect of making those marginal entities, which are particularly important in rural areas, non-viable financially. HHS ends by estimating that the average start up cost to a small entity will be $733 and the ongoing yearly cost will be $343. It is important to point out that these costs are based on all the assumptions and incalculable costs stated in the impact analysis, the accuracy of which have already been called into question.

F. Collection of Information Requirements

The Economic Growth and Regulatory Paperwork Reduction Act[274] requires HHS to estimate the hourly burden its regulation

271. *See id.* at 60038.
272. *See id.* at 60041.
273. *See id.*
274. *See* Pub. L. 104-208 (1996).

will impose.[275] HHS estimates a total yearly burden of 13,773,591 hours to comply with SPIIHI.[276] Unfortunately this estimate is subject to the same limitations as HHS' cost estimates discussed earlier this article. Out of ten sections of the rule, HHS is only able to estimate the time expenditures of six and even these seem low. Thus, as with the cost analysis, this hours estimate is merely the minimum amount of time that could possibly be spent complying with this rule and may be grossly inaccurate.

G. Federalism

Executive Order 12612 permits federal action limiting the discretion of state and local governments where, as HHS quotes, "constitutional authority for the action is clear and certain and the national activity is necessitated by the presence of a problem of national scope."[277] HHS asserts that "[p]ersonal privacy issues are widely identified as a national concern by virtue of the scope of interstate health commerce."[278]

There is no doubt that personal privacy issues are a local, state and, as HHS points out, a national concern. However the question of whether this national concern rises to the level of a "national problem" is not so clear. In quoting Executive Order 12612 as partial authority for the very broad scope of this rule, HHS fails to quote the next sentence of the order that is a cautionary modifier of the quoted sentence and reads:

> For the purposes of this Order: (1) It is important to recognize the distinction between problems of national scope (which may justify Federal action) and problems that are merely common to the States (which will not justify Federal action because individual States, acting individually or together, can effectively deal with them).[279]

Thus while HIPAA clearly orders the HHS to promulgate a rule, the question of whether the scope of the national concern presented by the perceived threat to privacy is sufficient to justify the scope of federal action suggested by HHS' rule is still open.

---

275. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 60045.

276. *See id.*

277. *See id.* at 60048 (quoting Exec. Order No. 12612 § 3(b) (1987)).

278. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 60048.

279. Exec. Order No. 12612 § 3(b) (1987), 52 Fed. Reg. 41, 685.

H. Unfunded Mandates, Environmental Impact and Coordination with Indian Tribal Governments

As discussed in section IV(D)(1), the Unfunded Mandates Act of 1995 requires a cost benefit analysis, which HHS combines with its impact analysis. In addition, the Act requires and HHS also provides an estimate of impact on national productivity, economic growth, full employment, job creation and exports. HHS first directly acknowledges that the long run costs of these privacy measures are likely to be passed on to patients.[280] It seems logical that an increase in the cost of health care will likely decrease utilization of health services, a decrease in economic growth at least in one sector of the economy. However, HHS explicitly states that it does not expect SPIIHI to have any substantial effect on productivity or economic growth. Indeed, HHS opines that SPIIHI may increase the numbers of persons seeking health care which will lead to a healthier population which will in turn increase national productivity and economic growth. Thus, a reader is left with the impression that SPIIHI could have a positive, negative or no effect on national productivity or economic growth.

In reality, there is probably no clear, rational way to predict SPIIHI's effect on overall national productivity or economic growth. HHS does plausibly predict that this proposal will result in some slowing of growth in traditional health care professions with an increase in fields assisting in compliance with the rule (legal professionals and management consultants).[281] On the surface, this seems a benign statement. In reality, this revelation foretells a shift of dollars originally designated to provide medical care into legal and administrative coffers, potentially a negative effect. HHS concludes its unfunded mandates analysis with the statement that SPIIHI will not likely affect exports and predicts SPIIHI will have no significant effect on the human environment.

Lastly, HHS indicates that it consulted with representatives of the National Indian Health Board, the National Congress of American Indians and the Self Governance Tribes.[282] Although the section states that questions about tribal autonomy and the status of tribal laws were discussed, it makes no mention of the

280. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 60044.

281. *See id.*

282. *See id.*

substance of those discussions.[283] Further, there is no mention of how SPIIHI would affect the poorer tribes that cannot now provide adequate healthcare for all of their enrolled members, yet will see dollars shifted from health care delivery to legal and administrative arenas.

V. The Burdens Imposed by HIPAA and SPIIHI and Issues Surrounding Those Burdens

Thus far, this article has highlighted two very fundamental flaws in SPIIHI: its failure to adequately define the privacy right it intends to protect and its failure to adequately analyze and assess the extent of existing and potential threats to health information privacy. In light of those flaws the paper has critically analyzed the enabling legislation (HIPAA § 264) and the proposed rule by which HHS intends to provide privacy protections (SPIIHI) stressing the breadth of the rule, its inconsistencies, and its potential cost. This analysis addressed four major issues surrounding SPIIHI: (1) SPIIHI's enormous cost; (2) the fact that SPIIHI may not really protect privacy at all; (3) other excessive burdens imposed by SPIIHI; (4) potential alternative solutions to enacting SPIIHI at this time. The remainder of this paper will discuss these issues and suggest alternative methods to achieve a reasonable level of privacy protection at an acceptable cost.

A. Constitutional Issues Surrounding SPIIHI

There are three separate constitutional issues connected with SPIIHI. The first is highlighted by the brevity of section 264 of HIPAA raising the question of whether Congress has unconstitutionally delegated legislative power to the executive branch by failing to provide adequate direction. The second question is whether HHS exceeded any authority properly delegated by Congress when it struggled to make SPIIHI as broad and inclusive as possible. The third subject is whether Congress' and HHS' intrusion into medical privacy protection without proper justification offends the principles of federalism. This section will address each of these issues separately.

283. *See id.*

1. The Legislative Mandate Delegated to HHS by HIPAA: Is it Constitutional?

A serious question arises regarding Congress' delegation of implementation authority to HHS in the event Congress fails to act. Crucial to this determination is an examination of SPIIHI through the lens of administrative law's "delegation doctrine" as currently interpreted by the Supreme Court. Although the United States Constitution reads "[a]ll legislative Powers herein granted shall be vested in a Congress of the United States,"[284] the Supreme Court has a long history of permitting the Congress to delegate significant portions of its legislative power to administrative agencies.[285] The logic behind this interpretation is that the Congress does not have the time, resources or expertise to deal with the minute details of every policy it enacts and oversees. These delegations have become so commonplace since FDR's New Deal that the administrative arm of the executive branch of government has been called a fourth, separate branch of government comprising the "dynamo of the modern social service state."[286]

While Congress clearly has the authority to delegate some part of its legislative function to administrative agencies, the limits of that judicially overseen privilege are not precisely delineated.[287] Thomas Jefferson recognized and drew a line generally by observing that the Congress should focus on "great" rather than "small" concerns.[288] However, what rises to the level of "great concern" and what is merely a "small concern" has been argued for more than two hundred years, with the precise position of the line changing as the composition of the Supreme Court varied.[289]

In Section 264 of HIPAA, Congress itself implicitly recognized that the task of developing health privacy standards was a "great concern" belonging principally to the legislative branch of government by requiring HHS to submit recommendations to

284. U.S. CONST. art. I, § 1 (emphasis added).

285. *See* Wayman v. Southard, 23 U.S. 1 (1825) (permitting Congress to delegate certain powers, while retaining those which must be entirely regulated by the legislature).

286. Jaffe, *An Essay on Delegation of Legislative Power*, 47 COLUM. L. REV. 561, 592 (1947).

287. *See Wayman*, 23 U.S. at 15-16.

288. *See* THE WRITINGS OF THOMAS JEFFERSON 424-425 (P. Ford ed. 1894).

289. *See generally* K. DAVIS, ADMINISTRATIVE LAW TREATISE §2.6 (1994); *see also* ALFRED C. AMAN JR., ADMINISTRATIVE LAW 9-39 (1993).

help Congress accomplish its legitimate task.[290] Congress properly retained explicit control over this legislative duty for thirty-six months, but, despite multiple attempts, failed to accomplish its task within its self imposed limit. This failure triggered HIPAA Section 264(c)(1) which automatically, summarily, and arbitrarily transferred Congress' clearly recognized duty to the executive branch of government.[291] Under Section 264(c)(1), Congress ordered HHS, without any further guidance, definition of terms, or discernible standards to do the legislative work it originally and legitimately reserved to itself. Thus a task which was unquestionably a "great concern" and belonged to the legislative branch of government at 11:59 PM on August 21, 1999, somehow became a "small concern" abruptly delegated to HHS at 12:01 on August 22, 1999. This action raises the very fundamental question of whether Congress provided sufficient direction to allow a constitutional basis for HHS to write this privacy rule.

Congress was correct in its original implicit recognition of the legislative nature of writing medical privacy laws. Even the primary drafter of the SPIIHI, John Fanning, senior policy analyst at HHS, recognized that this process should be accomplished legislatively, not administratively, saying that "legislation is the correct way to provide the provision."[292] Unfortunately, after the self-imposed Congressional time limit expired, HHS and Mr. Fanning seemed to conclude that they had no choice but to follow the Congress' explicit though misdirected mandate for HHS to take over the job.

The fact that HHS produced the rule, however, does not make it constitutional. That is a question that can ultimately be answered only by the Supreme Court. The delegation of legislative authority to administrative agencies may be a time honored process that has generally been given wide deference by the Su-

290. *See* Pub. L. No. 104-191 §264.
291. See id.
292. Cassie M. Chew & Mark Felsenthal, *Clinton Releases Proposed Regulation, Officials Stress Limits on HHS' Authority*, 8 BNA HEALTH LAW. 1747, 1748 (1999) (quoting John Fanning speaking at a teleconference on privacy and security issues in health care sponsored by the American Bar Association's Health Law Section on Oct. 29, 1999).

preme Court,[293] but the Court has set some limits to what Congress should delegate.[294]

These limits are particularly well articulated by the Court in *Eastlake v. Forest City Enterprises, Inc.*, which said "[c]ourts have frequently held . . . that a congressional delegation of power to a regulatory entity must be accompanied by discernible standards, so that the delegatee's action can be measured for its fidelity to the legislative will."[295] In *Arizona v. California,* the Court made the specific point in relation to agencies that consensual government requires that "the fundamental issues in our society will be made not by appointed officials but by the body immediately responsible to the people."[296] More recently, in *Miseretta v. United States* the Court said, "we long have insisted that the integrity and maintenance of the system of government ordained by the Constitution mandates that Congress cannot delegate [in entirety] its legislation power to another Branch."[297]

Perhaps the current jurisprudence of the Supreme Court in this area is best summarized by Professor's Aman's eloquent statement in his administrative law hornbook:

> By consensus, it is a proper thing for Congress to identify social problems and work through the rudiments of a solution, and then to turn the program thus established over to an agency and its professionals for implementation: knowing that within this frame of things the agency gains a portion of lawmaking power. It is, however, quite another thing for Congress not to legislate in some primary manner, but instead to turn to an agency to say, "Here is the problem, deal with it." Today this maneuver is likely to be seen as an unacceptable passing of the buck, the buck being Congress's responsibility under Article I for important choices of social policy. That important choices of social policy ought to be made in Congress – and not by unelected officials and a bureaucratic pro-

293. *See e.g,* Arizona v. California, 373 U.S. 546 (1963) (allowing the secretary of the interior considerable authority over the apportionment of water from the Colorado River based on the fact that the statute outlined factors which the secretary was supposed to consider when executing his duties). For examples of what is considered to be sufficient guidance for delegation of Congressional power to pass Congressional challenge, see *Lichter v. United States*, 344 U.S. 546 (1948) and *Miseretta v. United States*, 488 U.S. 361 (1989).

294. *See* Yakus v. United States, 321 U.S. 414, 426-27 (1944); Amalgamated Meat Cutters v. Connally, 337 F.Supp. 737 (D.D.C. 1971). *But see* Federal Energy Admin. *v.* Algonquin *SNG*, 426 U.S. 548 (1954).

295. 426 U.S. 668, 675 (1976) (emphasis added).

296. 373 U.S. 546, 626 (1963) (emphasis added).

297. 488 U.S. 361, 371-72 (1989).

> cess – seems a requirement of article I and an implication of the Constitution's profound regard for consensual government.[298]

This author is simply unable to glean even a minimal "discernable standard" from the half page, three hundred word provision of HIPAA to support the Constitutionality of a six hundred page document affecting a 1.3 trillion dollar market and broadly revolutionizing how medical data is handled and protected. Congress' implicit admonition that "individual medical privacy is threatened, fix it" is insufficient to pass muster as the "discernable standard" necessary for constitutionality. Further, although the Supreme Court has permitted delegation of legislative authority when Congress has explicitly deemed an agency better equipped to handle certain details, it is unlikely to accept the argument that a task initially explicitly reserved to Congress itself can become constitutionally delegable based on the passage of time rather than the enunciation of adequate guidelines.

The process of defining and balancing competing interests in our government has always been considered primarily the province of elected representatives. The more complex the issues and the more divergent the conflicting interests, the more important it is for the final compromises to be worked out on the legislative battlefield. Thus, reinforcing Congress' original position on privacy rules is the reality that issues of medical privacy and the protection of IIHI are among the most complex imaginable. They include individual patient interests in autonomy, control, discrimination and dignity; societal interests in medical research and advancement, disease prevention, ensuring the availability of medical care to the population, law enforcement and the cost of medical care; and interests of the commercial sector including insurers, pharmaceutical companies, hospitals, providers and many others. Addressing these myriad interests requires defining the right to privacy, deciding what parties have a legitimate interest in IIHI, determining a rank order for those legitimate interests, analyzing how the right to privacy might be invaded by non-legitimate interests, and finally achieving an affordable and workable compromise between these multiple issues. In the case of medical record privacy, the legislature is clearly the proper arena to accomplish this process. While it is true that the delegation doctrine has rarely been used to sweep-

298. Aman, *supra* note 289, at 12-13.

ingly nullify legislation, in this instance it is a real possibility that the Court would strike Congress' seemingly unfettered delegation to HHS.

2. SPIIHI's Scope of Regulation: Is it Constitutional?

A judicial corollary of the "delegation doctrine" is the principle that an administrative agency performing its function of legislative rulemaking cannot exceed the authority properly delegated to it by Congress. Assuming, arguendo, that HIPAA's delegation of authority to HHS was declared constitutional, SPIIHI still faces constitutional challenge in that it arguably exceeds the authority Congress delegated.

The Supreme Court has used the "delegation doctrine" as a canon of interpretation to prevent agencies from exceeding delegated powers. It has done this in two types of cases: (1) when it found the agency was making decisions with inadequate data; and (2) when it found an agency was serving too narrow an interest.

The classic illustration of the first form of judicial control is the "Benzene" case, *Industrial Union Dep't., AFL-CIO v. American Petroleum Inst.*[299] Here the Supreme Court struck down as unconstitutional an OSHA decision attempting to reduce workplace exposure to benzene (a known carcinogen) to extremely low levels based on minimal data. OSHA claimed the authority to balance the interests of potential death (however remote) due to workplace exposure with productivity concerns, totally ignoring potential costs.[300] The Court denied OSHA that authority finding that such power properly resided in the legislative arm of government unless explicitly delegated.

An example of an agency serving too narrow an interest can be found in *Hampton v. Mow Sun Wong*.[301] In *Mow Sun Wong*, a Civil Service Commission (CSC) regulation barring non-citizens (including lawfully admitted resident aliens) from employment in the federal competitive civil service was held unconstitutional, as servicing too limited a set of interests.[302] Although *Mow Sun Wong* is primarily a case about due process rights, the Court stated that the federal power over aliens was

299. *See* 448 U.S. 607 (1980).
300. *See id.* at 646.
301. *See* 426 U.S. 88 (1976).
302. *See id.* at 117.

not so plenary that any agent of the Federal Government could arbitrarily subject all resident aliens to different substantive rules from those applied to citizens.[303]

Through HIPAA, Congress clearly delegated the authority to protect electronic information handled by certain covered entities. HHS in analyzing its task found that simply following this mandate would have left so many loopholes as to make the legislation meaningless. Rather than re-present this problem to Congress and request guidance, HHS' solution was to stretch its constitutional authority to close the loopholes. In doing so, as in *Benzene*, HHS assumed a non-delegated power: the power to balance a "right to privacy" (note that this right is created in the rule and not the enabling legislation) with the working efficiency of the American medical system. Also similar to Benzene, the justifications for this claim of sweeping power are rooted in non-scientific data (surveys, anecdotes, rumor, innuendo, and sound bites) insufficient to support such an action factually. As in *Mow Sun Wong*, HHS balances one very narrow interest, the right to privacy, against an extremely broad field of interests.

Unfortunately, by following this course, HHS exceeded its constitutional bounds in at least two important areas. The first area is the type of records protected. HIPAA only intended to protect electronic records. Even President Clinton recognized that HHS did not have the authority to regulate paper records, stating in a press release accompanying the SPIIHI that only an act of Congress could extend coverage to all paper medical records.[304] However, HHS constructed a complex system of record keeping that makes it nearly impossible to economically separate paper records from electronic records, thus creating a system that *de facto* regulates all paper medical records. This exceeds its constitutional authority.

The second area that HHS exceeds its delegated authority is in reference to the entities it attempts to cover. Congress, in HIPAA, specifically defined the entities it intended to regulate, restricting them to health plans, health care clearinghouses, and to any health care provider "who transmits health information in electronic form in connection with transactions referred to in

303. *See id.* at 88.

304. Chew & Felsenthal, *supra* note 292, at 1748 (quoting President Clinton on Oct. 29, 1999).

section 1173(a)(1)."[305] Again, concerned over loopholes, HHS decided to capture the business partners of covered entities by requiring contractual provisions and holding covered entities responsible for the business practices of partners beyond their legal control. This provision not only oversteps the explicit authority granted by HIPAA, it also invades the province of the states to regulate insurance contracts.

Following Supreme Court jurisprudence in *Benzene* and *Hampton v. Mow Sun Wong*, it seems unlikely that the present Supreme Court would support the constitutionality of SPIIHI. HHS has simply taken too many liberties to vindicate too narrow an interest with too little objective data and minimal attention to cost.

3. Federalism Issues: Are They Fatal to the Constitutionality of SPIIHI?

If, as seems logical, HHS intends to regulate common law privacy protections, it must find a rationale for doing this that does not offend the Commerce Clause. In the "proposed need" section noted briefly above HHS discusses a "philosophical or common-sense" perception of the need for privacy protection and, in other sections throughout the preamble, it alludes to the Commerce Clause as the means by which the HIPAA statute and SPIIHI have the right to regulate privacy in the commercial arena.[306] This gives the impression that HHS intends to invade the province of a state to protect the welfare of its citizens through the back door of the Commerce Clause. However, HHS fails to explicitly state and justify this intrusion thereby threatening the precepts of federalism.

There is certainly ample precedent for federal protection of citizen welfare using the Commerce Clause but these protections have generally required a clear showing of a impending

305. *See* HIPPA, Pub. L. No. 104-191 §262(a), 110 Stat. 1936, 2023 (1996) (codified at 42 U.S.C. § 1320d-1).

306. "Personal privacy issues are widely identified as a national concern by virtue of the scope of interstate health commerce." Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59918, 60048 (1999) (proposed). "We are proposing this approach because we believe that it focuses most directly on the primary concern raised by HIPAA: the fact that growing use of computerization in health care, including the rapid growth of electronic transfers of health information, gives rise to a substantial concern about the confidentiality of the health care information that is part of this growing electronic commerce." *Id.* at 50028.

threat.[307] A significant flaw in HHS' argument is that there is no clear demonstration of an imminent hazard. Instead of providing hard statistical data about real damages caused by the misuse of IIHI, HHS has focused on anecdotal reports and surveys to show that fear of privacy violation is a major concern. In doing so, it has failed to show that injury from privacy invasion is an actual, manifest threat.[308]

HHS' failure to provide objective data about actual rather than potential individual damage as a basis for the remarkably broad scope of SPIIHI and its failure to specifically define how it is using the Commerce Clause to reach regulation of IIHI may prove a constitutional barrier to enforcement. Originally, when wielding the Commerce Clause the federal government was required to demonstrate a direct connection to and impact upon interstate commerce to justify impinging upon state jurisdiction.[309] However, since the late 1930s and early 1940s, the United States Supreme Court has been liberal in holding that the Commerce Clause may serve as the basis for the federal government to invade the police powers reserved to the states.[310] Most recently, though, in *United States v. Lopez*,[311] the Court considered the extent of interstate involvement in determining

307. *See* Heart of Atlanta Motel, Inc. v. United States, 379 U.S. 241 (1964) (holding the Commerce Clause is sufficient, itself, to give Congress the power to regulate private hotels since each house of Congress is replete with findings that black citizens found it difficult to travel because of a lack of accommodations available to them, thus interfering with interstate travel and commerce).

308. "Clearly, the growing problem of protecting privacy is widely understood and a major public concern. Over 80 percent of persons surveyed in 1999 agreed with the statement that they had 'lost all control over their personal information.' A Wall Street Journal/NBC poll on September 16, 1999 asked Americans what concerned them most in the coming century. 'Loss of personal privacy' topped the list, as the first or second concern of 29 percent of respondents. Other issues such as terrorism, world war, and global warming had scores of 23 percent or less. The regulation is a major step toward addressing this public concern." *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. at 60010. *See also infra* Parts III-IV.

309. *See* NOWAK AND ROTUNDA, *supra* note 36, §§ 4.1-4.7.

310. *See e.g.* Wickard v. Filburn, 317 U.S. 111 (1942). In that case, an Ohio farmer raised wheat on 23 acres of land. He consumed most of the wheat on his farm, either by feeding it to livestock, making flour for personal use, or using it to produce seeds for future crops. The Secretary of Agriculture assessed a penalty against the farmer for exceeding his allotment for planting under a federal statute regulating wheat production. The Supreme Court upheld the assessment, holding that the Congress's limitation of the farmer's wheat production was a valid exercise of its authority under the Commerce Clause to regulate interstate commerce. Unless *Wickard* is read narrowly, very little that occurs in this country can be viewed as not having some involvement with interstate commerce.

311. 514 U.S. 549 (1995).

whether oversight of an activity is within the bounds of Congress's authority. In *Lopez*, the Supreme Court, for the first time in sixty years,[312] struck down an act of Congress, the Gun-Free School Zones Act,[313] on the basis that the act exceeded congressional commerce clause authority. The Court held that it was inappropriate to make an excessively elastic application of the Commerce Clause.[314] It stated that for an economic activity to come within Congress's authority under the Commerce Clause the activity must "substantially affect" interstate commerce.[315] Since *Lopez*, at least eleven Federal courts in four separate circuits have similarly limited Commerce Clause authority.[316] If the United States Supreme Court is unwilling to allow Congress to invade the state's rights to decide how best to protect children from guns on school yards, is it likely to find the protection of potentially embarrassing information a more compelling need?

Thus, to summarize the multiple constitutional flaws in SPI-IHI, Congress, when it drafted HIPAA, failed to provide adequate direction in delegating to HHS the legislative authority to entirely revise the medical industry's handling of medical records in the name of privacy protection. HHS then overstepped any authority HIPAA arguably conferred in drafting the regulations so broadly. Lastly, HHS offended federalism by failing both to adequately define the privacy interest it intended to protect and to provide objective data about the actual threat it has a national interest in protecting.[317] These failures makes it

312. See Edmond Seferi, *FAA and Arbitration Clauses—How Far Can It Reach? The Effect of* Allied-Bruce Terminix, Inc. v. Dobson, 19 CAMPBELL L. REV. 607, 617 (1997).

313. *See* The Gun-Free School Zones Act, 18 U.S.C. § 922(q)(2)(A) (1988) (making it a federal crime "for any individual knowingly to possess a firearm that has moved in or that otherwise affects interstate or foreign commerce at a place that the individual knows, or has reasonable cause to believe, is a school zone").

314. *See United States v. Lopez*, 514 U.S. 549, 559 (1995).

315. *Id.*

316. *See* Westlaw, Key Cite *United States v. Lopez*, 514 U.S. 549, 558-59 (1995).

317. In *Lopez*, Chief Justice Rehnquist divided previous Commerce Clause cases into three categories of permissible regulation, any of which could arguably reach the regulation of IIHI. These categories include: instrumentalities of interstate commerce (laws regulating safety of vehicles used in interstate commerce – the computer is the vehicle by which IIHI is moved across state lines); channels of interstate commerce (laws freeing channels of commerce from discrimination, immoral activities, or injurious uses – misuse of information is potentially injurious); and activities having a substantial relation to commerce (regulation of healthcare information may have a substantial effect on the ability of companies to do business in a cost effective way). *See Lopez*, 514 U.S. at 558-59. To be on safe Constitutional grounds, HHS should

unlikely that SPIIHI could withstand constitutional scrutiny by the current Supreme Court because there is no well defined federal interest to balance against the intrusion into state affairs.

B. Costs: Is SPIIHI a Cost Effective Way to Spend America's Health Care Dollars?

Of the added burdens placed on patients, providers and the healthcare system in general, the financial strain of implementing SPIIHI is clearly the most significant. HHS admitted that the cost for implementation will be passed on to the consumer.[318] Interestingly, though, for a revolutionary program that goes beyond any privacy protection currently in place in this country, there is little substantive justification for the expenditures and no exhaustive cost estimate.[319] In fact, HHS' efforts have been categorized by some critics as "ephemeral and subjective."[320]

Nevertheless, HHS did estimate that the total cost of SPIIHI would be $3.8 Billion for five years, an estimate that is undoubtedly significantly low due to the unsophisticated model used to predict cost and the fact that when expenses were difficult to predict, HHS simply omitted them.[321] Most of the health care industry has been waiting for the regulations to be finalized before investing significant resources in accurate cost estimation models to counter HHS' assertions.[322] However, after a thorough reading of SPIIHI, the American Medical Association (AMA), American Hospital Association (AHA) and American College of Surgeons (ACS) all agree that HHS has substantially underestimated the cost of its regulation.[323] Blue Cross was suf-

---

have developed clear, concise arguments addressing HIPAA's constitutional (and consequently HHS' and SPIIHI's derivative authority) to regulate IIHI.

318. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59918, 60016 (1999).

319. *See* Brittin, et al., supra note 76, at 1956-57; *see also infra* Parts II and III.

320. *See* Rick Pollack, Executive Vice President, American Hospital Association, Letter to Donna E. Shalala commenting on the Proposed Standards for Individually Identifiable Health Information dated Feb. 17, 2000 at Broad Issues § I, available at <http://www.aha.org/ar/letters.asp?%6cookupLetterID=198> (visited Feb. 21, 2000).

321. *See supra* Part IV(D)(3)(b-g).

322. Telephone interview with John Supplitt, Senior Policy Analyst at the American Hospital Association, in Chicago, IL 2/17/00.

323. *See* Pollack, *supra* note 320 (stating that the AHA believes HHS has seriously underestimated the costs of implementation); *see also* Thomas R. Russell, Executive Director, American College of Surgeons, Letter to Margaret A. Hamburg dated Feb. 15, 2000, http://www.facs.org/about_college/acsdept/socio_dept/acs_comments/medrecconf.html (visited Feb. 21, 2000) (stating the College is skeptical of the cost

ficiently concerned about these costs that, in advance of the final regulations, it independently commissioned the Nolan Report which concluded that SPIIHI would cost $43 billion over five years, an order of magnitude higher than HHS' estimate.[324] Legal analysts have simply said, "the plan proposed will be burdensome and more expensive to implement than anyone likely contemplates."[325]

Another method to estimate SPIIHI costs might be to examine the complexity of SPIIHI in relationship to a similar endeavor of known cost. For example, hospitals spent an estimated $8.2 billion in two years on Y2K compliance.[326] Systems analysts estimate that the complexity of hospital changes required for SPIIHI may be two to three times as complex as those required for Y2K.[327] In addition to the reprogramming requirements, SPIIHI requires rewriting contracts, training staff, new policies and procedures, hiring consultants, notice requirements and many other costs. Examining SPIIHI through this lens suggests that the true costs may be much closer to the $43 billion than $3.8 billion.[328]

Whatever the exact dollar figure, the unfortunate conclusion regarding the price of SPIIHI is that HHS has presented a rule, the true cost of which is completely unpredictable except to say that it will be very expensive (at a minimum in excess of $10-20 billion dollars over five years and more likely $30-40 billion) and that the expenditure will reduce the funds available to actually deliver health care.

Further, HHS is promulgating this rule at a time when America is in the midst of a financial health care crisis. The delivery of health care already costs American citizens in excess of one trillion dollars annually, or approximately 15% of the

estimates); E. Ratcliff Anderson Jr., Executive Vice President, American Medical Association, Letter to Margaret A. Hamburg dated Feb. 17, 2000 at 43, available at http://www.amaassn.org/ama/basic/article/238-574-1.html> (visited Feb. 21, 2000) (stating the burden estimates are very inaccurate).

324. *See* Robert E. Nolan Company, *supra* note 50.

325. Chew & Felsenthal, *supra* note 292 (quoting Alan S. Goldberg, an attorney with the Boston Office of Goulston and Storrs).

326. *See* Pollack, *supra* note 320, at Broad Issues § III.

327. Personal interview with Ida Androwicz, R.N., Ph.D., acknowledged expert in the field of hospital informatics 2/24/00 at Loyola University in Chicago, Illinois.

328. Three times $8.2 billion ($16.4-$24.6 billion) plus extra costs of $10-$15 billion would total between $26 and $39 billion.

gross national product.[329] Despite this enormous expenditure, a significant segment of the population goes without adequate medical care. In fact, based on a realistic cost estimate, the price of SPIIHI's proposed privacy protections could pay to extend health care to every child in America or pay for a Medicare prescription drug benefit.[330] No law can, as SPIIHI attempts to do, provide total protection against every individual who is intent on misusing information. Thus, before enacting a privacy rule, it is important to ask the questions, (1) is the defined level of privacy protection really necessary and (2) is it worth the cost of decreased care to America's children and elderly?

For the past fifteen years state and federal governments have focused major efforts on the tasks of decreasing the growth rate of health care expenditures and finding ways to recover money misspent through overuse of the medical system or outright fraud and abuse. HIPAA was the federal response of that focus and has as a clear goal to both recover misappropriated funds[331] and to reduce expenditures through increasing efficiency.[332] SPIIHI with its attendant expenditures is in direct conflict with HIPAA's goals.[333] Its approach to reach, without clear justification and without adequate impact analysis, into hundreds of thousands of health care entities in thousands of locations, most of whom already have in place safeguards to protect confidentiality of patient information, is not only of questionable constitutional validity, it is also redundant and irresponsible. SPIIHI does not provide a cost-effective way to spend a defined portion of America's health care dollars on privacy protection.

329. *See* PROSPECTIVE PAYMENT ASSESSMENT COMMISSION REPORT AND RECOMMENDATIONS TO CONGRESS 12 (1996) (predicting yearly expenditures for health care will exceed 1.4 trillion dollars by the year 2000).

330. The estimated five-year budget for the Children's Health Insurance Program is $22 Billion. The estimated cost for the Medicare prescription drug benefit is $37 Billion for five years. *See* Robert E. Nolan Company, *supra* note 50, at 3.

331. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, Title II.

332. *Id.* § 261.

333. The AHA expressed this concern eloquently saying "the prescriptive nature of the proposed standards will require hospitals to rewrite policies, retrain staff, renegotiate contracts, and put in place comprehensive systems to track all uses and disclosures of information. Such changes are costly and conflict with the cost reduction goals of HIPAA." Pollack, *supra* note 320.

C. *Individual Rights: Who Does SPIIHI Really Protect and Is This Protection Needed?*

SPIIHI is intended to protect patients from the unconsented use of their private health care data. HHS accomplishes this goal by creating four new explicit and one new implicit "rights." However, it limits its protection to "covered entities," specifically health care providers, health care plans and health care clearing houses and generally omits protection from privacy invasion by the federal government.

The four explicit new rights SPIIHI creates for patients are: (1) the right to written notice of information practices; (2) the right to an accounting of how an individual's IIHI has been disclosed; (3) the right of an individual to obtain access to her own IIHI; and (4) the right to request amendment and correction of PHI.[334] Of these four rights, the first two are probably unnecessary and the last two can likely be created at a much lower cost.

The right to written notice of information procedures is a simply a waste of money in relation to any substantive benefit conveyed. In regard to notice, HHS makes note of its intent to "create a system where open and accurate communication between [covered] entities and individuals would become necessary and routine" by holding entities liable for the information practices they publish under the notice requirements of §164.512 which include both posting of a notice and delivery of a notice to the patient.[335] This statement exposes the presupposition that open and accurate communication does not exist between covered entities and patients. While this may be true for some entities such as insurance companies, it is unlikely true in physician offices.

Further, while notice requirements may be a reasonable way to shift the burden of ensuring that citizens are informed of their rights from a government agency to private industry, it is difficult for this author to understand how such a requirement will create new channels of open and accurate communication between physician and patient. Thus, the notice requirement is simply too broad to be cost effective.

Likewise, the right to individual accounting of how information has been disclosed by every covered entity is much more

334. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59918, 59976-59988, 60059-60062 (1999) (to be codified at 45 C.F.R. §§ 164.512, 164.514, 164.515, 164.516) (proposed).

335. *Id.* at 59951.

expensive than any conceivable benefit. In keeping with the theme that HHS should inform Congress that it cannot craft a reasonable rule given its delegated powers, these notice and accounting requirements should be abandoned in favor of a statement in the definitive legislation that Congress intends to protect individuals from misuse of IIHI as defined by the legislation and the requirement that all entities amassing IIHI on a significant scale keep track of such disclosures.

The rights to access and correct misinformation in health records are more substantive but for the most part do not require federal intervention. Most states already provide personal access to individual medical records from providers. If states find that their citizens need to be able to amend or correct records at a local level (hospital, physician or state databases), state legislatures can find a way to accomplish this. Federal law should be concerned with requiring the entities it licenses to gather and store large data sets of IIHI to allow inspection and review of that information. This could be accomplished inexpensively by requiring the entity to send a data report to a requesting individual for a reasonable fee, such as is currently required of credit bureaus. Similarly, any disputed information could be subject to an administrative review process allowing either correction of misinformation, a limited accompanying explanatory statement by the individual, or both.

In addition to the explicit rights, SPIIHI creates at least one implicit right. It creates the explicit duty to mitigate harm from inappropriate disclosure of PHI.[336] This duty gives rise to the implicit patient right to recover damages when that duty is breached. As written, however, SPIIHI contains no provision for individual legal action. If a licensed entity damages an individual, the individual should have either administrative or judicial recourse to recover those damages.

The issue of what entities SPIIHI protects the patient from is also an interesting one. SPIIHI only protects patients against privacy violations by a limited group of "covered entities." Conspicuously missing from this group of entities is the government itself, except in very narrow circumstances such as when it provides care. In light of the fact that the vast majority of federal privacy cases have been against the government, the rule again seems markedly misdirected at entities which already adequately protect patient data.

336. *See id.* at 60062 (to be codified at 45 C.F.R. § 164.518 (f)).

D. Other Burdens Imposed by SPIIHI

The previous section points out the three major problems with SPIIHI: its inherent unconstitutionality, high cost, and the fact that it is an inefficient guardian of the very rights it invents and ostensibly protects. There are numerous other unreasonable, detrimental and expensive burdens imposed by SPIIHI. This section will briefly enumerate some of the more important of those encumbrances.

1. Administrative Burdens related to Business Partners

In the struggle to extend control beyond entities specifically covered by HIPAA legislation, SPIIHI creates a major burden for covered entities by holding them liable for violations perpetrated by their business associates including billing firms, consultants, and attorneys.[337] In creating this liability, the Secretary goes so far as to require all covered entities to enter a contractual agreement with each business partner and offers a detailed list of mandates that must be set forth in those contracts. This is basically another attempt to expand the scope of the HHS' authority outside of HIPAA constraints.

The effect of this provision is to impose on business associates adherence to all of the provisions of SPIIHI, as well as compliance with the privacy policies and practices of the covered entities themselves. Business partners, in turn, would be required to impose similar contractual provisions upon any of their associates or sub-contractors to whom they disclose protected information. All of these entities would be expected to participate in compliance audits by HHS. Finally, the proposal states that material breaches by business partners of their obligations under the contract would be considered noncompliance on the part of the covered entities, if the covered entities knew or reasonably should have known of such breach and failed to take reasonable steps to cure the breaches or terminate the contracts.

These provisions place enormous administrative and legal burdens on covered entities and their business partners. For business partners that perform services for multiple entities, the proposed rule means they must implement multiple sets of information policies and procedures. For physicians and other covered entities, the proposed language means that they would be required to know the policies and procedures of the entire

337. *See id.* at 59947-59950.

universe of businesses with which they contract, or be held liable. This is a totally unrealistic and unworkable overstepping of constitutional authority by HHS.

2. Preemption

In accordance with HIPAA mandates, SPIIHI cannot preempt state laws that offer more protection, require parental notification or that relate to a wide variety of state functions.[338] HHS has put a positive spin on these restrictions saying that SPIIHI will create a federal floor of privacy protection. In reality however, these legislative restrictions prevent HHS from creating a nationally uniform rule that is equitably and cost efficiently enforceable. Not only is SPIIHI flawed, expensive and potentially unenforceable, it simply cannot do the job it is intended to do because of the size and number of loopholes.

3. Research Information

One of the most important areas in which SPIIHI creates additional burdens is the area of scientific research. While it is clear that Institutional Review Boards (IRB) are necessary protections for the rights of patients, SPIIHI expands the criteria that IRBs and other internal privacy committees must apply in approving a research proposal and its use of protected information. These additional requirements include: (1) the research must be impracticable to conduct without the PHI; (2) the research project is of sufficient importance to outweigh the intrusion into the privacy of the individual whose information would be disclosed; (3) there is an adequate plan to protect the identifiers from improper use and disclosure; and (4) there is a plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research. These requirements are imposed with absolutely no data or evidence that they are directed at remedying an existing problem and in the face of a well-established common IRB rule already adopted by seventeen federal agencies.[339]

Respected physician organizations have expressed concern that HHS is acting prematurely in imposing these new criteria, stressing that HHS has "not completed its planned review of the

338. *See* HIPAA § 262. For example, SPIIHI cannot preempt state laws relating to reporting of disease or injury, child abuse, birth, death, public health surveillance, regulatory reporting, state regulation of insurance and many others areas.

339. *See* Brittin et al., *supra* note 76, at 1955 n.52.

Common [IRB] Rule nor has the Institute of Medicine spoken to [the] issue."[340] These concerns highlight another major flaw in SPIIHI – the fact that it was issued without sufficient attention to its ramification or adequate consultation with the professional groups affected by the rule.

4. Compliance and Enforcement

SPIIHI requires that all covered entities comply within twenty-four to thirty-six months of the finalization of the rule and, because it lacks a private right of action, allots the entire enforcement burden to HHS. HHS has neither the staffing nor the fiscal resources to enforce such a broad and complex rule uniformly and equitably. The likely result will be haphazard, random and inconsistent enforcement which will not achieve the uniform minimal privacy protection HIPAA intended but will instead ignite a firestorm of litigation, again diverting precious health dollars into the legal and administrative stream of commerce.

VI. Alternatives to Enacting SPIIHI as a Final Rule: What Should HHS Do With SPIIHI

The two glaring conceptual flaws in SPIIHI[341] and the many major and minor blemishes in its drafting[342] raise the question of what should be done with HHS' massive document? If SPIIHI is allowed to take effect as written, the flurry of legal challenges trying to iron out the problems in a piecemeal fashion will likely result in the diversion of more precious health care dollars into the judicial system. On the other hand, if SPIIHI is simply scrapped, the hard work of Mr. Fanning and countless others would be wasted.

There are alternatives to scrapping SPIIHI or enacting it as written. The first is to simply take into account all the comments generated by the proposed rule and try to revise the final rule in light of those comments. A second would be to return to the legislature and ask for proper guidance and authority to

340. *See e.g.*, Russell, *supra* note 323.

341. The fact that HHS fails to define its ultimate goal adequately and coherently and the fact that its proposed protections are not focused on the existing problem. *See supra* Parts I and II.

342. The potential lack of constitutionality, the lack of cost concerns, the placement of a privacy right higher than a right to health care and other major burdens. *See supra* Part V.

write a meaningful rule. A third would be to seek substantive help from the industries involved to accomplish the stated goals.

In its commentary on SPIIHI, the American Hospital Association urged HHS to more carefully consider costs and other burdens it imposes and rewrite it, limiting its scope to the statutorily defined transactions before finalizing this regulation.[343] Similarly, the American College of Surgeons and American Medical Association also advised rewriting SPIIHI.[344] With proper deference to these three organizations,[345] merely rewriting a flawed document seems an exercise in futility. More time and money should not be wasted on this effort.

Alternatively, the proposed rule could serve as a starting point to generate legislative discussion to overcome the conceptual flaws and constitutional problems in the existing document. A rewrite of SPIIHI in light of the comments received could serve as the basis for a bill to properly delegate the constitutional authority necessary for HHS to construct meaningful rules. SPIIHI, in a modified form, could be sponsored by a bipartisan group of elected Senators and Representatives and introduced into the legislative arena as a bill to be debated, compromised and molded into a statement of discernable standards which can then be handed back to HHS to rewrite appropriate regulations.

The best solution would be for HHS to simply inform Congress that it cannot, given the legislative guidance and mandates provided, produce a set of constitutional rules that will accomplish meaningful protection of IIHI. There is no shame in admitting that the tools provided are inadequate for the job at hand. Then, HHS should take its medical advisory role to Congress seriously by first defining very carefully what aspects of medical record privacy should be protected on a federal level and what should be left to the states. Smaller scale issues of what occurs in a physician's office or an individual hospital should be left to state legislatures and courts to protect. They are already doing this, and for the most part, successfully. The bigger issue of large multi-state information warehouses amassing large amounts of medical data with high abuse potential

343. *See* Pollack, *supra* note 320, at Broad Issues § III.

344. *See* Russell, *supra* note 323; *see also* Anderson Jr., *supra* note 323, at 47.

345. The author is an individual member of two of the three organizations (the AMA and the ACS) and works for an organization which belongs to the AHA.

should be dealt with at a federal level in a more deliberate fashion.

HHS should make recommendations about how to protect IIHI only after defining and prioritizing specific threats to its confidentiality. It should then address the cost of neutralizing each threat individually so that Congress can make the proper cost/benefit and political interest balance analyses. The MIB, credit bureaus and other large data users are only collecting information because they find it financially beneficial. If carefully defined legitimate uses are permitted to continue but abuses are made financially detrimental, the misuse of IIHI will largely cease and the problem to shrink to a more manageable size.

Throughout his lifetime, Justice Brandeis was a key player in defining the right to privacy so perhaps it would be instructive to return to his principles to develop a regulatory scheme to protect it. Brandeis clearly believed that the best way to regulate information in the securities field was to make it available for inspection saying: "Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light is the most efficient policeman."[346] Without exposing actual IIHI to unnecessary inspection, Brandeis' principle may be applied to the practices of information collection and use. Instead of trying to micromanage IIHI, HHS should recommend that Congress simply make it illegal to amass data in relative secrecy such as is currently done by the MIB and credit bureaus.

The privilege of collecting large amounts of IIHI should require federal licensure and Congress should appropriate sufficient funds to allow HHS to be a watchdog over licensed companies to ensure the data is secure from misuse. Congress should further define the legitimate purposes for which such data can be used and institute sufficient penalties, civil and criminal, to make the misuse of IIHI financially non-viable. This plan, while requiring more creative thought and initial expenditure to define the problems, would be much more likely to be cost effective in the long run.

An alternative to the dilemma of what to do with SPIIHI is to call upon the various industries to be regulated to help write workable legislation and rules. This approach has been success-

346. *See* Natural Resources Defense Council v. Securities & Exchange Comm'n, 432 F. Supp. 1190, 1198 (D.C. Dist. Ct. 1977) (quoting Justice Brandeis from BRANDEIS, OTHER PEOPLE'S MONEY 92 (1932).

ful in other health care legislative endeavors. For example, when Medicare was charged with the task of developing standardized Medigap policies it turned to the National Association of Insurance Commissioners (NAIC) for help.[347] NAIC successfully developed ten options, defined by the benefit packages each offers, and submitted them to HHS which adopted the plans by reference.[348] Further, the NAIC, the American Medical Association, the American Hospital Association, the American College of Surgeons and others have already expressed an interest in assisting HHS in the task of developing privacy protections.[349]

In the case of SPIIHI, the process would be more complex and time consuming than that undertaken in Medigap. Medigap only covered one major type of organization–insurers–while SPIIHI intends to cover hundreds of types of organizations. To effectively obtain help with workable rules, HHS would need to appoint and convene at least five committees: (1) health care providers; (2) health care plans; (3) health care clearing houses; (4) governmental entities; and (5) consumers. Many of these committees would need multiple subcommittees to deal with the variations in businesses contained in each general grouping. For example, providers would need committees to look at the problems with hospitals, physicians, long term care facilities, etc.

There are two problems with this approach: cost and time. The cost could probably be absorbed to a large extent by the various groups who would likely perceive a chance to influence the process of developing cost effective rules for privacy protection as a good business investment. HHS would thus only have to support the consumer and government committees. Time is a significant hurdle in that a project of this size would likely take a minimum of two to three years to complete. However, the likelihood that a workable, cost effective and reasonable solution

347. *See* 42 U.S.C. § 1395ss (p) (1999).

348. *See* 42 U.S.C. § 1395ss (p) (1999) (giving the NAIC authority to develop the standardized plans and requiring that happen by 1991); *see also* Medicare Program; HHS' Recognition of NAIC Model Standards for Regulation of Medigap Policies, 57 Fed. Reg. 37980 (1992) (where HHS actually adopts the NAIC model policies) and Medicare Program; Recognition of NAIC Model Standards for Regulation of Medicare Supplemental Insurance, 63 Fed. Reg. 67078 (1998) (updating the NAIC model policies to comply with the Balanced Budget Act of 1997).

349. *See* Meg Fletcher, *NAIC Seeks Privacy Input*, BUS. INS. March 27, 2000 at 1; *see also* Russell, *supra* note 323; Anderson Jr., *supra* note 323; Pollack, *supra* note 320, at Broad Issues § III.

would come out of the process offsets any negative implications of the time investment.

To most effectively implement this plan, the consumer committee should be convened first to establish and rank in order of importance what privacy violations should be regulated. It should also establish what percentage of the total dollars available for medical care should be expended to ensure that privacy. This list and cost determination should then be turned over to the four other committees and their subcommittees to develop cost effective procedures to implement necessary controls. HHS should oversee the entire process and then help Congress draft appropriate enabling legislation to allow HHS the proper constitutional authority to enact the proposed rules. In terms of enforcement, HHS should retain the ability to police the system but should also provide a private right of action to allow citizens to recover personal damages.

CONCLUSION

In summary, HHS, in response to the mandates of section 264 of HIPAA, has drafted a proposed rule on privacy protection that is flawed and totally unworkable. The rule fails to adequately protect the intended privacy interests at an exorbitant cost in an unconstitutional fashion. It has major defects in its conception in that it fails to adequately define the privacy it intends to protect or clarify the threat to medical information confidentiality. The rule then proposes to spend an incalculable but enormous sum of money on that protection, exceeding its delegated authority and offending concepts of federalism without proper justification. Lastly the rule imposes expensive burdens in many ancillary areas such as research and contracting without any regard for the fact that these burdens will reduce the amount of medical care delivered to groups in desperate need of care.

The last paragraph may sound like a damning criticism of HHS but it is not intended to be read in that light. HHS was handed an unconstitutional mandate and made a Herculean effort to comply with that mandate. However, the task is simply not possible with the tools provided by Congress. At this time, the final rule should be suspended until HHS adequately addresses the concerns of the many physicians, providers and insurers that have critically analyzed this rule. It should refuse to act in an unconstitutional manner and demand adequate gui-

dance from Congress. In the meantime, HHS should consider bringing industry, government and patients together to develop a creative and cost effective proposal that will afford protections to consumers and give them a right to hold violators responsible for damages caused by misuse of private medical information while not overzealously diverting their health care dollars into administrative and legal channels.