Privacilla.org

Your Source for Privacy Policy from a Free-market, Pro-technology Perspective

Health Privacy in the Hands of Government:

The HIPAA Privacy Regulation — Troubled Process, Troubling Results

A Special Report Issued by Privacilla.org
http://www.privacilla.org

April, 2003

Introduction

Dramatic changes to health care administration are underway in the United States thanks to a new regulation issued by the U.S. Department of Health and Human Services. The regulation, issued under the Health Insurance Portability and Accountability Act, purports to advance the universal goal of protecting the privacy of patients in the American health care system.

But nothing is simple when it comes to privacy. And nothing is straightforward when it comes to the HIPAA privacy regulation. The regulation was issued under an unusual law in which Congress abandoned power and responsibility for health policy to federal bureaucrats. Neither Congress nor the Department of Health and Human Services ever defined privacy before seeking to protect it, dooming the effort somewhat from the start.

Privacy is important — health privacy even more so — and health itself is an essential good. Privacy should not conflict with cost-effective care. But government estimates put the cost of the HIPAA privacy rule at 17 billion dollars, and private estimates go much higher. HIPAA compliance has become a profit center for lawyers, lobbyists, technology vendors, consultants, and many others. The flurry of economic activity is nice, but dollars spent on HIPAA compliance will not go to treating sick children or keeping prescription costs down for seniors. The American public should demand demonstrable improvements in their privacy for this cost.

The threats to health privacy that exist today are a symptom of deeper problems in the health care system, such as the growth of third-party payers. True solutions will come from reform of the health care market overall. In the meantime, regulations aimed at privacy can only hit their mark if policymakers understand basic concepts like privacy itself. They must understand the protections that already exist for privacy in the society and in our law.

Congress and HHS did not do their homework before embarking on this health privacy excursion. More political gamesmanship than policymaking went into the privacy provisions of the HIPAA law. The regulators ignored a substantial web of existing privacy protections and constructed a complex regulatory contraption out of whole cloth.

The final HIPAA privacy regulation contains a variety of crisscrossing and overlapping policies, some of which even conflict with privacy. Overall, it reduces consumers' power to demand privacy from health care providers on the terms they want, replacing consumer power with a uniform federal regulatory regime. This is not an advance, but a retreat for privacy. Now that another feckless regulatory intervention aimed at privacy has failed, perhaps true study of health privacy can begin.

Systemic Threats to Health Privacy are a Symptom of Deeper Problems

There are reasons why health privacy seems so at risk today, and why consumers feel so disempowered in terms of health information and health care choice as a whole. To see them, one must look at the whole field.

True health privacy relies on empowered patients choosing among options made available to them by providers competing to serve them. This happens in hearty markets, where sellers vie with one another to discover and deliver whatever consumers want. But the American health care system is not well. Concerns about health privacy are a symptom of a much larger disease.

Third-Party Payers Stand Between Patients and Doctors

The major culprit is the persistence and continuing growth of third-party payers in the health care market.[1] Third-party payers are institutions that stand between patients and doctors to fund health care. They come in two major forms — employer-provided health insurance and government health insurance such as Medicare and Medicaid.

Most Americans have health insurance that is provided by their employers rather than having insurance they purchase for themselves. Employer-provided health insurance is a relic of World War II, during which price controls prevented employers from paying higher wages. They responded by offering insurance as a non-wage benefit.

Health benefits are a deductible business expense for employers. No similar tax deduction is available to people who buy their own insurance. This creates a strong tax bias in favor of employer-provided health care, and it has persisted and grown. Tax policy has warped the market for health insurance so that individuals cede authority over health insurance decisions to employers.

Over-Insurance Hides Costs from Patients, Driving Costs Up

Because employers' health plan decisions are typically made by or for executives who are advanced in age and supporting families, the average corporate health plan is relatively generous, with low or no deductibles and minimal co-payments. This means that the average worker, who is younger and supports fewer dependents, is over-insured.

For relatively young, healthy people, the more appropriate insurance policy has a relatively high deductible. It protects against major calamity and extended illness, leaving day-to-day health care to be paid for out-of-pocket. But many workers are almost fully insulated from the cost of their health care.

Likewise, patients without private health insurance are often covered by government health insurance such as Medicare or Medicaid. These people also pay only

[1] *See generally* Stan Liebowitz, *Why Health Care Costs Too Much*, June 23, 1994 (Cato Institute Policy Analysis No. 211) < http://www.cato.org/pubs/pas/pa211.html>.

a portion of the actual costs of the medical resources they use. Very few people actually pay their entire health care bills, though some portion of the country's "uninsured" have actually made the rational, if risky, choice not to insure because they are unlikely to need significant medical care (and because they can fall back on government-provided care if the choice turns out to be error).

The natural result of insulating people from the costs of their health care choices is excessive demand for health care services. People will naturally take more of something that is offered to them cheaply, or for free. As in any market, excessive demand for health care services drives prices up. But, unlike in a normal market, patients do not respond to price cues and ratchet back on unnecessary treatments; they do not know what the prices are. This is one important part of a health care cost spiral, a spiral that ultimately threatens health privacy.

Third-Party Payers Use Personal Health Information to Push Back

In both the employer- and government-provided health insurance contexts, the patient is not the customer of the doctor or hospital. Rather, the patient is the beneficiary of an arrangement by the government or between the employer and the insurer. Rather than going to the doctor, dollars in hand, to buy health care, the patient goes to the doctor and simultaneously applies to the health plan to request payment for the treatment.

As health care costs have continued to spiral upward, both government and employer-sponsored plans have had to become stingier about what services they cover. Without the discipline that consumers show with their own dollars when they have appropriate, high-deductible health insurance, plans must increasingly review whether patients are seeking appropriate care. To do this, they must investigate the medical conditions, treatments, and prognoses of individual patients. They must use patient information to study the cost-efficacy of treatments.

In these poorly functioning health care markets, third-party payers oversee choices that patients would otherwise make in confidential consultation with their doctors. This opens up reams and reams of otherwise private health information.

Poor tax policy and government entitlements have driven government agencies, employers, and insurers to become voracious consumers of health information. Fixing tax policy and restraining government entitlements will restore the discipline of market processes to our health care system. It will empower consumers, lower costs, and reduce the current anti-privacy bias created by third-party payer systems.

The HIPAA privacy regulation came to a health care market that is falling further and further out of whack and taking on an increasing bias against privacy. Fixing the market would fix much of the bias. Congress should have done this long ago, and it remains unfinished business.

The Concept of Health Privacy Can and Should be Understood

Congress should also have captured the concept of privacy before it began the wheels of regulation rolling with the HIPAA law. It is essential to define privacy, though almost no policymakers or advocates have done so. This leaves Americans not knowing when they have privacy, and when they do not. It means that policymakers may spend enormous sums and heap costly regulation on consumers not knowing whether their programs and policies advance or retard privacy. Privacy is a definable, knowable concept, even if it is not simple.

The term "privacy" has long vexed policymakers, businesspeople, and consumers because, in casual conversation, it is used to describe any number of concerns with the modern world. People express concerns about crimes like identity fraud as a "privacy" problem. They often intermingle privacy with security — a much larger, overarching concept. They treat unwanted advertising as a "privacy" problem, even though spam and telemarketing come from sellers who know little or nothing about people, but presume to contact them anyway.

Defining Privacy

Privacy is a state of affairs individuals experience having to do with the amount of personal information about them that is known to others and on what terms. Specifically defined, privacy is the subjective condition that people experience when they have power to control information about themselves and when they have exercised that power consistent with their interests and values.

Foremost, privacy is a subjective condition. It is individual and personal. One person cannot decide for another what his or her sense of privacy is or should be. Likewise, government regulation in the name of privacy can only create confidentiality or secrecy rules based on the guesses of politicians and bureaucrats about what "privacy" should look like. Such rules can only crudely ape the privacy-protecting decisions that millions of consumers would otherwise make in billions of actions and transactions every day.

The Role of Law

An important factor in this definition of privacy — power to control information — essentially goes to the influence of law. Law determines whether people are empowered to protect privacy.

Law has dual, conflicting effects on privacy. On one hand, it protects the privacy-enhancing decisions people make — by enforcing contracts, protecting bodily integrity and property rights, and so on. A body of U.S. state tort law also directly protects privacy, giving anyone in the possession of sensitive personal information the responsibility to protect it and use it tactfully, if at all.

On the other hand, law often undermines individuals' power to control information. Many entitlement and tax programs show how the helping hand of government strips away privacy before it goes to work. Government demands for personal information of all kinds are tremendous and growing.

The Role of Choice

Perhaps the most important, but elusive, part of privacy protection is consumers' exercise of power over information about themselves consistent with their interests and values. This requires consumers and citizens to be aware of the effects their behavior will have on their privacy, and act accordingly.

Technology and the world of commerce are rapidly changing, and personal information is both ubiquitous and mercurial. This makes relationships between personal information, behavior, and privacy difficult to catalog, even for full-time students of information policy.

Though it may be difficult to exercise, consumers in a free market always have the power and choice to absent themselves from privacy-invading transactions. There is an active advocate community, a watchdog press, and a variety of government bodies that are constantly educating the public and looking for privacy violations. Though many of them are also seeking to impose their privacy preferences rather than letting consumers decide, their work advances market solutions all the same.

Privacy is delivered when people have the power to control information about themselves and when they use that power in ways they want. Americans make a wide variety of choices about personal information. Some affirmatively seek publicity for information about themselves that others view as gravely personal — on the *Jerry Springer Show*, for example. Our assumptions, and the conventional wisdom about privacy, are as often wrong as they are right. This is as true in health care as in any other field.

Understanding Health Information

A variety of assumptions and presumptions are built into the HIPAA privacy regulation and the debate about health privacy generally. They should be brought into the light of day.

The first deals with scope. Health information is more than just transactions subject to the HIPAA privacy regulation, of course. Health information can be just about anything — from the fact that a person has acne, a cold, or a broken leg to the fact that a person has an incurable sexually transmitted disease, or that a person will soon die. To diagnose or treat health conditions, a wide variety of intimate personal information is often needed — living arrangements, sexual preferences, allergies, habits, medical history, and so on. Much information that is commonly not sensitive or private is also needed, such as body type, race, age range, allergies, habits, physical appearance, and so on.

Discussions of health privacy often start from the premise that health information is extremely private and sensitive. And that is sometimes true. Many people keep certain facts very tightly held, sharing it only with doctors, close relatives, and loved ones. But others consent to have their conditions, surgeries, and treatments broadcast on national television and the Internet.[2] More commonly, people relish the attention, flowers, phone calls, and cards they receive when an illness or injury is publicized. Privacy varies in thousands of ways from individual to individual and from circumstance to circumstance.

Health information is a broad swath of information that ranges widely from highly sensitive to unremarkably mundane. From individual to individual, the sensitivity of health information varies widely, as well. It would surely be difficult to capture the true health privacy interests of hundreds of millions in a single, national regulatory regime. Better, it would seem, to disperse protections, and move responsibility for them, to people who are close to the action — like doctors and patients. This is how health privacy protection worked before the HIPAA privacy regulation.

A Web of Health Privacy Protections Predated HIPAA

Protections for health privacy existed before the HIPAA privacy regulation. After all, *something* was restraining doctors, hospital administrators, and health plans from widely broadcasting patient information before HIPAA.

Indeed, more than a half dozen separate social and legal regimes protect privacy in different ways. Each one alone is insufficient protection, but woven together they can provide substantial privacy assurance to patients — without expensive, top-down government mandates on the health care system.

Ethics and Professionalism

Doctors and other medical professionals should be offended by some of the documents produced by HHS during the HIPAA privacy rulemaking. In breathless, faux urgency about the lack of privacy protection for health records, HHS cast aside the professionalism and ethical obligations of this calling.

Doctors, nurses, medical technicians, and medical office administrators are highly educated and trained professionals. They help individuals deal with some of their most helpless, and most hopeful, times in life. They are highly attuned to the social context of disease and healing. As a rule, they understand the expectations of patients and society for sensitive treatment of health information. They did not need federal regulation to tell them to serve patients' privacy needs.

---

[2] *See, e.g.,* One Man's Experience of Healing From Cancer Web site <http://www.christopher-sheppard.com/health.htm>.

But more than good breeding and habits goes into the medical profession's privacy-protective culture. The Hippocratic Oath includes a privacy-protective admonition. In the classical version, it is: "What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about."[3] In the modern version: "I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know."[4]

The American Medical Association has an active Council on Ethical and Judicial Affairs.[5] Its nine Principles of Medical Ethics include the following: "A physician shall respect the rights of patients, colleagues, and other health professionals, and shall safeguard patient confidences and privacy within the constraints of the law."[6] From the time they are students to the end of their careers, the overwhelming majority of medical professionals take these obligations seriously.

By largely ignoring ethics and professionalism as an important privacy protection, regulators in Washington have sullied the practice of medicine. Doctors are not privacy-insensitive rubes who need oversight from the real professionals in the federal bureaucracy. And Washington, D.C. does not have a lock on the dignified practice of medicine.

State Medical Licensing Boards

Ethics, professionalism, and trust are not empty words, of course. They are backed up by institutions that control a physician's ability to practice. Ethical duties of confidentiality are enforced by state medical boards.

State medical boards are typically organizations of volunteer medical professionals who regulate the practice of medicine and limit it to qualified personnel. They often operate under state statutes, usually called a Medical Practice Act.

The Federation of State Medical Boards includes privacy protecting requirements in its model Medical Practice Act. Boards are authorized to take disciplinary action for unprofessional or dishonorable conduct against physicians who "willfully or negligently violat[e] the confidentiality between physician and patient . . . ."[7]

---

[3] *See* The Hippocratic Oath: Text, Translation, and Interpretation, by Ludwig Edelstein. Baltimore: Johns Hopkins Press, 1943, *excerpted at* <http://www.pbs.org/wgbh/nova/doctors/oath_classical.html>.

[4] *Attributed to Louis Lasagna, Academic Dean of the School of Medicine at Tufts University, and excerpted at* <http://www.pbs.org/wgbh/nova/doctors/oath_modern.html>.

[5] *See* AMA Council on Ethical and Judicial Affairs Web site <http://www.ama-assn.org/ama/pub/category/2498.html>.

[6] American Medical Association, *Principles of Medical Ethics* (June 2001) <http://www.ama-assn.org/ama/pub/category/2512.html>.

[7] Federation of State Medical Boards, *A Guide to the Essentials of a Modern Medical Practice Act* (9th Edition) § IX(D)(8) (April 2000) <http://www.fsmb.org/Policy%20Documents%20and%20White%20Papers/9th_edition_essentials.htm>.

Few doctors are punished by medical boards for violating privacy, because few doctors violate privacy. Doing so can be harmful to a career — whether a medical board takes action or not.

Markets

When a doctor, insurer, hospital, or health system has violated privacy — or even come close — people talk. Patients talk to each other. Doctors talk to neighbors. Nurses talk to friends. Newspapers and reporters talk to communities. Competing health systems talk to the privacy violator's customers. Reputations are made and reputations are lost. No market relies more heavily on reputation and trust than health care.

An active privacy advocate community, a watchdog press, and legislators and law-enforcers constantly hover over the business community looking for privacy violations. Each one they turn up teaches the whole community about flawed privacy practices. Privacy gaffes are keenly watched for by the business community. Privacy officers learn from them and study ways to ensure that their companies will not be next.

Hundreds of privacy protective practices are infused into the health care field by practitioners responding to consumer demand. Rightly or wrongly, health care providers can be drummed out of communities and out of business if they do not provide privacy on the terms consumers want.

The workings of the marketplace in channeling behavior are so obvious and everyday that they sometimes go without mention. Each dollar a consumer spends with one provider over another rewards the first and punishes the second. Nationwide, consumers issue many trillions of pinpricks and pats on the back each year. Privacy is one of the many factors they consider.

This process should not be ignored. It is a powerful social force that helps deliver privacy.

Contract

Nearly every commercial exchange occurs based on a contract. A contract is the agreement between people or businesses to exchange things of value. In the case of medicine, it is usually the exchange of money for advice and treatment.

A contract exists whether there is a written document or not. When a contract is unwritten, or when the written terms of a contract are incomplete, courts will infer those terms from the behavior of the parties, customary practice, good public policy, and other sources. Medicine is no exception. Contracts for professional services, such as law, medicine, financial planning, and the like, have long had confidentiality as either an implied or explicit term.

Confidentiality has been found an implied contract term by courts in cases where patients have accused medical practitioners of wrongly sharing confidential information. Patients have successfully sued health care providers for violating the health care contract.

In a New York case called *Doe v. Roe*,[8] for example, the former patient of a psychiatrist sued because the psychiatrist had published a book reporting verbatim detail about the patient's thoughts, feelings, emotions, fantasies, and biography. The court found for the patient and held that "the physician-patient relationship is contractual and in it there is implied the physician's promise to obey the Hippocratic Oath," citing the confidentiality provision of that oath.[9]

Every health care treatment is provided on terms that are laid down in a contract. The terms include privacy protection. The vast majority of treatments go off without a hitch and the role of contract is forgotten. Contracts protect privacy — by law — and this fact should be held up to the light. It is an important part of the legal web of privacy protection.

Malpractice

Much more law protects health privacy. As discussed earlier, doctors and other medical professionals are ethically obligated to protect patient confidences. The promise of confidentiality is an important part of developing the trust that leads to successful treatment.

Thus, failure to protect privacy exposes doctors, hospitals, and health systems to lawsuits based on malpractice. In the case of *Watts v. Cumberland County Hospital System*,[10] for example, a patient brought an action against a marital and family therapist, charging that he had persistently discussed her treatment with others both during and after the course of treatment. The court of appeal found that the suit was best characterized as a medical malpractice action because of the therapist's professional misconduct.[11]

The failure to provide confidentiality can be a failure to provide competent professional treatment. The threat of malpractice liability protects privacy.

Other Health-Specific Legal Theories

[8] 93 Misc.2d 201, 400 N.Y.S.2d 668 (N.Y. Sup. Ct. 1977).
[9] *Id.* at 205.
[10] 75 N.C.App. 1, 330 S.E.2d 242 (1985).
[11] *Id.* at 9.

Other theories of liability exist when doctors or health systems have revealed patient confidences.[12] The right to sue has been premised on the general public policy that offensive and shocking behavior is actionable. The physician-patient legal privilege may give the patient a right to sue when confidences are breached. State licensing statutes may give patients a cause of action when the physician violates it. And courts may find that physicians have a fiduciary duty to their patients.

There is no lack of privacy law specific to the health care field. But there is general law too.

The Privacy Torts

The privacy torts protect sensitive information on any subject, and on any medium. (Indeed, they applied to the Internet from the first moment it was used.) They represent a general, legally-backed duty that people holding sensitive information have to safeguard it and use it tactfully.

Tort law is a type of state law that gives people the right to sue if they have been harmed in ways that the law recognizes. Over more than a hundred years, a group of privacy torts have evolved and been adopted in nearly every one of the United States.[13]

The privacy torts give people who have suffered privacy invasions the right to sue on a variety of theories. The most important in the medical treatment context is the "disclosure" tort, which is committed when someone wrongly reveals embarrassing personal information about another.

The privacy torts adjust automatically to the varying sensitivity of information in varying contexts. Health information is often more sensitive than other information, and the privacy torts naturally require those in possession of such information to take greater care with it. The essence of compliance with this law is tact and common sense.

Importantly, the privacy torts do not dictate the practices that will protect privacy, as regulations almost always do. There are no required privacy disclosures or forms to sign. And they certainly do not permit or encourage disclosure of information for purposes that federal bureaucrats deem appropriate.

Rather, the privacy torts say to people possessing information: "Do no harm." Under the tort regime, creative people are allowed to discover innovative new uses of information that are consistent with the privacy of consumers. The privacy torts allow all

[12] *See* Hammonds v. Aetna Casualty & Surety Company, 243 F. Supp. 793 (N.D. Ohio 1965); Horne v. Patton, 291 Ala. 701, 287 So.2d 824 (1973); Humphers v. First Interstate Bank, 68 Or. App. 573, 684 P.2d 581, 587 (1984); MacDonald v. Clinger, 84 A.D.2d 482, 486, 446 N.Y.S.2d 801, 804 (1982).

[13] *See* The Privacy Torts: *How U.S. State Law Quietly Leads the Way in Privacy Protection*, Privacilla.org (July, 2002) <http://www.privacilla.org/releases/Torts_Report.html>.

beneficial uses of information and punish only harmful ones.[14] Tort law provides substantial privacy protections, even if pro-regulation privacy advocates and regulators purposefully ignore it.[15]

Long before the HIPAA law passed, there was an overlapping web of ethics, incentives, and legal protections for privacy. Each one alone is imperfect, but combined they are significant.

Yet privacy and existing protection for it were almost totally alien concepts to Congress when it passed the law that authorized the HIPAA privacy regulation. The story of how it ducked its responsibility to learn these concepts is a fascinating study in politicking and sleight of hand.

The Source and History of the HIPAA Regulations

In 1996, the growth of the Internet and the beginnings of e-commerce were fomenting new worries about privacy. Some Members of Congress, still red-faced about the collapse of the Clinton Administration's health care plan, were eager to grow the federal government's role in health care. Senators Kennedy (D-MA) and Kassebaum (R-KS) joined together to pass a substantial law called the Health Insurance Portability and Accountability Act.[16]

Rather than fixing the underlying causes of privacy threats like the third-party payer problem, however, Congress thought it should attack privacy head on. Or so it may seem to people who are unaware of what Congress actually did.

Faced With a Difficult Problem, Congress Punts

Congress did not take steps to protect privacy in the HIPAA law. Instead, it wondered aloud what privacy was and how it should be protected. The privacy section of HIPAA was called "Recommendations with Respect to Privacy of Certain Health Information,"[17] in a subtitle called "Administrative Simplification." This section asked

---

[14] The HIPAA privacy regulation bans all uses of covered health information unless it is approved. Over time, this will prove a serious hindrance to innovation, needlessly costing Americans life and longevity.

[15] In December 1999, when it promulgated its sweeping regulation of health care information practices under HIPAA, the Department of Health and Human Services mentioned the existence of the privacy torts twice, even noting that state tort law allows patients to hold health care providers accountable for some unauthorized disclosures of health information. But it relied on and quoted a study by the Institute for Health Care Research and Policy at Georgetown University to find that "'state laws, with a few notable exceptions, do not extend comprehensive protections to people's medical records.'" The study came to this conclusion by specifically excluding state common law and the privacy torts. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,461 (2000), quoting Health Privacy Project, Institute for Health Care Research and Policy, Georgetown University, *The State of Health Privacy: An Uneven Terrain* 17 (1999) http://www.georgetown.edu/research/ihcrp/privacy/statereport.pdf.

[16] Pub. L. No. 104-191 (2nd Sess.) <http://aspe.hhs.gov/admnsimp/pl104191.htm>.

[17] Pub. L. No. 104-191, § 264 <http://aspe.hhs.gov/admnsimp/pl104191.htm>.

the Secretary of Health and Human Services to make recommendations to Congress about the privacy of individually identifiable health information. Congress asked HHS what rights people should have with regard to such information, the procedures that should be used to enforce those rights, and the uses and disclosures of such information that should be authorized or required.

This law went several steps further than asking a federal agency for recommendations, though. It told the Secretary of HHS to go ahead and write into law whatever the recommendations were if Congress did not act.

Delegations of authority like this are terrific politics. The Members of Congress who passed HIPAA can take credit for passing the law *and* retain complete deniability for the HIPAA privacy regulations. From constituents who like the regulation, they can collect praise. With constituents who do not like it, they can point their fingers at the bureaucrats in the Department of Health and Human Services. But delegating authority and responsibility to a federal agency for political ends is only the beginning of the story.

Good Politics Makes Bad Policy

The timeline of the HIPAA privacy regulation shows how political gamesmanship can trump good policymaking. Comparing HIPAA's legislative and regulatory schedule to the nation's political schedule reveals the close relationship between good politics and bad policy.

Congress enacted the HIPAA law in August 1996. The November presidential election contest between Bill Clinton and Bob Dole was just ahead. HIPAA called for the privacy recommendations to come exactly twelve months later. The recommendations would come, of course, from a Department of Health and Human Services controlled by the winner of that election.

The new President would also be able to veto any privacy legislation coming from Congress after the HHS had issued its recommendations. If Congress passed a health privacy law that did not perfectly meet the President's preferences, he could veto it and issue his own regulation. In other words, instead of seeking the consensus required by the processes laid out in the Constitution, Republican and Democratic leaders put federal health privacy policy down as a bet on the 1996 election race. Democrats won the bet.

Predictably, Congress failed to act. One of the terms of the bet, in that case, was that the Department of Health and Human Services would issue privacy regulations "not later than" 42 months after HIPAA was enacted. According to the law, the regulations would have been issued in December 1999, less than a year before the next presidential election in the year 2000.

This timing is important because the party that won the original HIPAA bet would still have to answer to voters in the 2000 election. This was an important restraint on

what would come out of the process because a privacy regulation that went too far in any direction could be a political issue and harm the party putting it forward.

But the Clinton Administration's HHS welshed on this part of the bet and did not issue the HIPAA privacy regulation until December 2000 — just *after* the election contest between George W. Bush and Al Gore. This allowed the Clinton Administration to issue a privacy regulation with minimal political risk for the Democratic party or any candidate for office.

A Constitutionally Flawed Process

Though one can never know whether it changed the substance of the regulation, this timing of it sheltered the Administration and the political party responsible for the privacy regulation from accountability to voters. This is no small irony given that it was a product of the "Health Insurance Portability and *Accountability* Act."

Politicians in both parties deserve substantial blame for their gamesmanship with federal health privacy policy. Federal law should be the result of consensus among elected representatives in Congress and the approval of the President. The HIPAA privacy regulations did not emerge from a process like this.

For this reason, the HIPAA privacy regulation may be constitutionally defective under the "non-delegation doctrine" which prevents Congress from ceding its power to the Executive branch, the Judiciary, or the private sector. Courts are reluctant to enforce this doctrine, but the regulation is a genuine contender to be being stricken on this ground.

The HIPAA law and the HIPAA privacy regulation came from a badly contorted political process. It should not be surprising that the results in terms of privacy are unclear and controversial. Rather than lifting a national burden, the multi-billion dollar mandate on the health care system may have no benefit, or even harm the privacy and confidence of American patients.

HIPAA Created as Many Privacy Threats as it Addressed

The latter half of the 1990s saw an upsurge in concern about privacy that coincided with the growth of the Internet. Many of the information practices that were at the center of this new concern had been evolving for decades, but the Internet and e-commerce gave them a new, public face.

A worthwhile national conversation continues today about how information moves in this Information Age. Heightened awareness of personal information and privacy among a broad swath of the public is a good thing, even if the ultimate reaction of most consumers is to ratify existing information practices because of the benefits they provide.

Privacy concerns about health care are distinctively *not* a product of the growth in online commerce. In June 2001, well after the HIPAA law was passed, the Congressional Research Service called the nation's health care system "largely paper-based and unstandardized."[18] It cited a Department of Health and Human Services estimate that about 400 different formats for electronic health care claims were then in use in the United States. Health care is only a small and slowly becoming a part of dot-commerce.

Thus, even as late as 2001, health information was somewhat protected from exposure by continuing "practical obscurity." Practical obscurity is when information that might otherwise be available is obscured because it is difficult to obtain and copy. Health information in paper files, or in electronic formats that are not interoperable, is relatively protected because it can not be passed willy-nilly among different users on different computer systems.

One of the goals of the broader HIPAA law was to eliminate the inefficiency created by incompatible electronic formats. The "Electronic Transactions and Code Sets" regulation created standards for the content and format of common health care transactions and named standards-maintenance organizations to keep them updated. In seeking to create efficiency, it began the elimination of practical obscurity in health records. This increased the threat to privacy and the specter of combined, poorly secured databases of Americans' health information.

The reality of a combined national health database moved a step forward with the HIPAA law, as well. HIPAA required the Department of Health and Human Services to adopt standards for a unique national individual health identifier. A national health ID so presages a national health database that Congress has consistently refused to fund the program. Nevertheless, the national health ID remains the law of the land. If and when Congress fails to prevent it, it will go forward. An effort to permanently eliminate the national health ID is underway.[19]

There is no question that standards for communication of health data will allow efficiencies into health care administration. But in HIPAA, Congress forced them on a health care market and a public that may not have been ready for their implications in terms of privacy. Congress also created a national health ID system that continues to loom.

As industrial policy for the U.S. health care industry, HIPAA largely overlooked the privacy interests of consumers. It eroded privacy as much as it may protect it. The privacy provision in HIPAA was a band-aid for a wounded health privacy that HIPAA itself injured further.

---

[18] CRS RL30620 Pg. 2

[19] *See* Letter from Congressman Ron Paul to House Appropriations Committee Members, March 28, 2003 <http://www.nccprivacy.org/paul-medid-2003.txt>.

HHS' Privacy Recommendations and the Path to Regulation

The initial privacy recommendations that HHS issued under the HIPAA law were true to the HIPAA law's origins. Congress had not identified the interest it intended by invoking the word "privacy" and the agency took that as permission to run free. It produced a document cheering for legislation that cut across a variety of information policies and interests. Among those was the government's interest in *reducing* Americans' health privacy.

The report[20] put forward five broad "principles" for federal legislation. These start to illustrate the direction that the final privacy rule would take — or, rather, the lack of direction it would take. Each of the categories is interesting and important, but they range widely across the information policy landscape:

- Principle 1: Boundaries — This was the idea that "[a]n individual's health care information should be used for health purposes and only those purposes . . . . It should be easy to use information for those defined purposes, and very difficult to use it for other purposes." A principle like 'boundaries' is hard to argue against, because it is meaningless.

- Principle 2: Security — HHS summarized this concept as protecting information against "deliberate or inadvertent misuse or disclosure." Security is a very important field in information policy, but it is much bigger than privacy. Without security, privacy can not be assured, just like the ability to make payroll or protect trade secrets can not be assured. Curiously, security was both a key "privacy" recommendation in this document and the subject of a separate "security" rulemaking under the HIPAA law.

- Principle 3: Consumer Control — "Patients should be able to see what is in their records, get a copy, correct errors, and find out who else has seen them." While these things are important and interesting, their tie to privacy is unclear. A medical record encased in concrete and thrown to the bottom of the deep ocean, for example, can not be accessed or corrected, but it is very private. This principle of "consumer control" goes not to privacy, but to fair and accurate treatment.

- Principle 4: Accountability — "Those who misuse personal health information should be punished, and those who are harmed by its misuse should have legal

[20] Confidentiality of Individually-Identifiably Health Information: Recommendations of the Secretary of Health and Human Services, Pursuant to Section 264 of the Health Insurance Portability and Accountability Act of 1996 <http://aspe.hhs.gov/admnsimp/pvcrec.htm>.

recourse." This principle also ranges well beyond privacy to any misuse of health information.

- Principle 5: Public Responsibility — "Individuals' claims to privacy must be balanced by their public responsibility to contribute to the common good, through use of their information for important, socially useful purposes . . . ." This fascinating "privacy" principle articulates a wide variety of reasons why people should *not* have privacy. The detailed list produced by HHS included health oversight, public health purposes, research, emergencies, to maintain state health data systems, to provide information to next-of-kin, for directories, for law enforcement to use against third-party payers, for law enforcement to use against individuals, for use in judicial proceedings, and so on.

Importantly, the HHS report also assumed the non-existence of safeguards for privacy. The only mention of the many privacy protections that exist came in a few cryptic lines buried deep in the report: "Some current enforcement of privacy rights occurs through litigation under common law theories of a general public policy of medical confidentiality . . . , contract, malpractice, and tortious invasion of privacy."

The report did not analyze how well medical ethics, explicit and implied contract rights, malpractice claims, or the state privacy torts protect privacy in health information. It did, however, advocate eliminating some of these protections.

With Congress failing to act on medical privacy legislation before the self-imposed deadline in the HIPAA law, the Clinton Administration went ahead and issued a proposed health privacy regulation. The proposed rule it issued in December 2000, like the initial HHS report, ignored existing privacy protections in pursuit of a wide range of information policies.

Early in 2001, the new Bush Administration re-opened the regulation for additional comment. There was much anticipation and clamor on the part of interests who thought the regulation did too much or not enough. Ultimately, the Secretary of Health and Human Services announced that the agency would go forward with the regulation on the same timeline, subject to some modifications. The modifications were issued in August 2002 and the rule took effect for most entities on April 14, 2003.

The Regulation: A Jumble of Policies, No Improvement in Privacy

The appendix to this paper summarizes and analyzes the HIPAA privacy regulation in terms of true privacy. It finds a jumble of different information policies with no clear vision for the improvement of Americans' health privacy.

The centerpiece policy — access and correction — is an important interest with many subtleties, but it is not a privacy interest. Indeed, access is tension with privacy

because it creates the opportunity for fraudulent access, and all manner of dastardly behavior, including privacy invasion.

Unsurprisingly, the regulation has a "one-size-fits-all" quality. Privacy is uniquely unsuited to being captured in a single, nationwide policy. Our people and their interests are too diverse. And health information ranges from acidly sensitive to drearily mundane depending on not millions, but billions of different health care circumstances that arise throughout the nation every year. The largest, smartest coterie of bureaucrats could not figure out all the right answers, and they have not.

Many policies found in the regulation are new and untested. The requirement to keep an accounting of disclosures, for example, is relatively novel, and its consequences are unknown. Along with creating real discipline (in terms of security, at least), the requirement may dissuade specialists from engaging in ad hoc research about new treatments, devices, and therapies. The loss will quietly accrue to American patients as they miss out on life-saving and life-extending discoveries.

The concept of "de-identified" information — as defined by an 18-point test — seems likely to become a playground for regulators. As new advances in information management develop, new requirements for de-identification will come forth. Rather than placing the risk and responsibility for preventing privacy invasion squarely on health care providers, the regulation will start a moving-goalposts game between providers and regulators. The definition of what "de-identifies" information will shift and jump, while compliance burdens will stay consistently high.

Most importantly, the regulation represents a seismic shift from privacy by contract to privacy by regulation. Many elements of the regulation copy the contract-forming process by giving patients certain options and forms to sign. But there is an increasing likelihood that contract will go away as a principle protection for patients. It will be replaced by regulations whose terms are formed not by doctors and patients, but by "experts" in Washington, D.C.

Reducing the role of contract in health privacy protection is a step in the wrong direction. Today, patients can and do ask doctors to treat certain information with special confidentiality, or provide treatments without making records of them. These privacy-tailored practices are likely to wane under the HIPAA law because high civil and criminal penalties are threatened for health care providers that HHS finds in violation of its rules.

The encroachment of federal regulation into this area moves control of health privacy decisions away from patients, not toward them. Power over health care has not moved from HMOs to patients, but rather from HMOs to the federal government.

This is made most clear by the enforcement and compliance provisions. Patients who are aggrieved by the privacy practices of a health care provider under the HIPAA privacy regulation can only complain to the Department of Health and Human Services.

Whether that agency pursues their interests will be a matter of dumb luck and skillful lobbying rather than justice and empowered consumerism. The solution to this problem is not to create private causes of action based on federal regulation, but a return to contract-based privacy protection.

More weaknesses in the HIPAA privacy regulation will surface as doctors, hospitals, and health systems try to implement all its provisions. Already, it is clear that the regulations have failed in an important respect: there is no sense in the land that the privacy of health information is any greater after HIPAA than before it. The promise of the HIPAA privacy regulation is not being delivered.

This represents a quiet tragedy, because compliance with the regulation will divert resources from the provision of actual health care to sick and dying patients. In a real sense, diverting at least 17 billion dollars from treatment will shorten lives and cause needless suffering. For this price, the American people should demand clear, robust privacy protections.

Conclusion

The story of the HIPAA privacy regulation is full of contradictions and Orwellian newspeak. In a law called the Health Insurance Portability and *Accountability* Act, Congress abandoned all accountability for federal health privacy policy. In a provision called "Administrative Simplification," HHS injected globs of muddy bureaucracy into an already complicated health care administration system.

Before the HIPAA privacy regulation, a web of ethics, incentives, and laws protected privacy. None alone was sufficient, but combined they were substantial. They were far too quickly dismissed in the HIPAA process, and their survival after HIPAA is in some doubt. HIPAA largely replaced a flexible web of privacy protections with a singular, breakable federal regulation.

When the HIPAA privacy regulation was first proposed, the Department of Health and Human Services cited several justifications for the regulation. Many of the privacy breaches it cited resulted from simple mistakes, or violations of existing law or rules. For example, it cited the accidental posting of medical records on the Internet by a health system; theft and misuse of HIV records by an employee (subsequently fired) of a city health department; an incident where health insurance claims forms blew out of a truck; and prescription records being found on the hard drive of a used computer.

Occasional privacy lapses are common in a land of nearly 300 million people — aberrations of all kinds are "common" — but the ability of federal regulation to prevent aberrational mistakes and criminal behavior is far from proved.

What we do know is that the cost of health care will rise to meet the cost of implementing the regulation. This cost will be paid in lives of American patients, their

comfort, and their happiness. For that price, the HIPAA privacy regulation should have delivered simple, clear protections for privacy. It should have lifted the burden of concern that rests on the shoulders of patients. It did not. In terms of actual results — privacy assurance for American patients — the HIPAA privacy regulation has already failed.

Appendix: The HIPAA Privacy Regulation Analyzed

On the pages that follow, the major provisions of the HIPAA privacy regulation are summarized and analyzed in terms of privacy. Many elements of the HIPAA privacy regulation go to interests other than privacy. And those focused on privacy have unclear — sometimes even negative — effects.

The text boxes contain summaries of the regulation combined from two Congressional Research Service reports: *Health Information Standards, Privacy, and Security: HIPAA's Administrative Simplification Regulations* (June 14, 2001)[21] and *A Brief Summary of the Medical Privacy Rule* (February 14, 2003).[22] The December 2000 rule is the original one issued by the Clinton Administration. The August 2002 rule is a series of amendments to the original that were made by the Bush Administration.

The lynchpin of the rule is this language: "A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter." [164.502(a)] In other words, all is forbidden unless it is permitted. This is the reverse of the general rule in free societies that all is permitted unless it is forbidden.

Covered Entities

Applies to health care providers who electronically transmit health information in connection with any of the HIPAA-covered transactions, health plans, and health care clearinghouses. [160.102, 164.500]

Privacy and health privacy do not begin and end with commercial transactions, of course. People's health privacy concerns may extend well beyond the regulation's "covered entities." Through the standardized transaction and code set rules, though the HIPAA law increased threats to privacy from the health care system. And the regulation ratifies disclosure of information to governments and government-approved entities for a variety of reasons.

The HIPAA law does bind federal and state government entities that fall within the definition of "covered entity," like the Medicare program, but other agencies that have personal health information are not covered. The Privacy Act, which protects many federal government data collections, is increasingly regarded as a paper tiger that lacks meaningful protection for personal information.

[21] C. Stephen Redhead, *Health Information Standards, Privacy, and Security: HIPAA's Administrative Simplification Regulations*, Congressional Research Service report #RL30620 (June 14, 2001).
[22] Gina Marie Stevens, *A Brief Summary of the Medical Privacy Rule*, Congressional Research Service report #RS20934 (February 14, 2003).

Covered Health Information

Applies to personally identifiable health information created or received by a covered entity and transmitted or maintained in any form or medium (e.g., paper, electronic, or oral) [164.501]

Though the coverage of the Act is generally unremarkable, it draws into its sweep and treats as private health information that may be obvious to everyone or widely known, such as visible skin conditions or injuries that are widely known to a community. This criticism is a nitpick but it illustrates the "one-size-fits-all" character of a federal regulation that tries to control literally billions of different facts about people's health in millions of different circumstances.

Patient Access

Gives patients the right to access, inspect, and copy their health information within 30 days of making a request for access, if the information is maintained or accessible on-site (otherwise within 60 days). Allows covered entities to impose reasonable cost-based fees for copying the information. Covered entities may deny access under certain circumstances. [164.524]

Access is often touted as an element of privacy, but a brief hypothetical illustrates how it differs: Imagine a patient's health record encased in concrete and dropped to the bottom of the deep ocean. The patient can not have access to it, nor can anyone else. The *privacy* of the information in the record is well protected even though access is impossible.

Access is actually in tension with security and, through security, privacy. An organization that is required to share records opens itself and the records to fraudulent access. A perpetrator of identity fraud may use personal information about his or her victim to gain access to medical information and do even more dastardly mischief, including privacy invasion and potentially dangerous interference with medical treatment.

The risk of privacy invasion and other harms is increased, not decreased, by access rights. Accordingly, the rule includes a regulatory standard for confirming the identity of patients — yet another of many complexities created by the access requirement.

Access to information may serve a variety of other values, such as accuracy of information and fair treatment. This is important in the health context, just like it is in other fields. It is also important for health professionals to maintain records that are not available to patients so that they may record honest observations and judgments without destroying patients' trust. Whatever the answer to these difficult problems, access is not a privacy protection.

Amendment of Health Information

Gives patients the right to request amendment of their health information and requires covered entities to act on such a request within 60 days. Allows covered entities to deny a request if they determine that the patient's information is accurate and complete, or was not created by the covered entity. Permits requester to submit a written statement of disagreement with the denial. [164.526]

Like access, the right to amend health information is important, but it is not a privacy protection. Like access, the right to amend creates security risks that can be life-threatening if used by criminals. Accurate health records are important to ensure proper treatment, in both the medical sense and for purposes of insurance, employment, and so on.

The stakes are very high in the area of access and amendment — so high that Congress should have analyzed all the tensions in this area separately, rather than abdicating responsibility to federal regulators purporting to deliver "privacy."

Accounting of Disclosures

Gives patients the right to receive, within 60 days, an accounting of disclosures over the past 6 years, except for disclosures for treatment, payment, and health care operations, and for certain other specified purposes. Accounting must include a brief statement of the purpose of each disclosure and the address of the recipient of the information. [164.528]

Required accounting of disclosures is an uncommon new information policy. It shares the risk of fraudulent use that access and amendment requirements have but it can provide a patient with important information for investigating privacy invasion or other wrongdoing.

Required accounting of disclosures may have any number of practical effects on health administration and medicine: Health systems are likely to develop stringent security and accounting practices, which is good. On the other hand, they are likely to restrict beneficial disclosures because of the potential liability. Specialists who want to compare the results of a new device or technique across a range of patients may be inhibited from reviewing records because of the bureaucratic hurdles to doing "official" research and their own legal liability from being on the "disclosed to" list of a patient whose treatment ultimately fails.

Patient Notice

Requires covered entities to provide patients with written notice of their privacy rights, as well as notice of the entities' legal duties and privacy practices. Specifies content of the notice. [164.520]

The August 2002 rule adds a new requirement for health care providers with a direct treatment relationship, that they make a good faith effort to obtain an individual's written acknowledgement of receipt of the provider's privacy notice.

Notice is widely regarded as a lynchpin of privacy protection, but more is assumed about notice than is known.

In the margins, notice may be beneficial because a small minority of consumers probably actually read information policies and notices. These highly concerned consumers (and those with too much time on their hands) probably gain some modicum of knowledge from them.

But a majority of consumers probably do not read privacy notices. The consensus holds that the billions of notices mailed out by financial services providers under the Gramm-Leach-Bliley Act went unread, doing more to kill trees than help consumers. The HIPAA privacy rule requires obsessive detail. This makes it less likely that they will be useful to consumers.

Likely, the majority of consumers make choices in the marketplace based on custom, brand, reputation, and so on, rather than the details of particular notices. Privacy advocates, the media, and government officials have a role in informing the public by highlighting suspect information practices, but consumer choice about information practices — including the need for affirmative or advance notice — should rule the day.

Minimum Necessary

Requires covered entities to make a reasonable effort to use or disclose the minimum amount of information necessary to accomplish the intended purpose, except for disclosures related to treatment. [164.502(b); 164.514(d)]

The August 2002 rule exempts from the minimum necessary standards any uses or disclosures for which an authorization has been received.

Disclosing "minimum necessary" information is a good practice. However, a "minimum necessary" requirement appears to spring from the idea that tight control over facts protects privacy. It does — if no facts are available, privacy can not be invaded.

But practical protection of privacy relies on tactful use of information by trustworthy and responsible parties. It may protect privacy in some small respect for an insurer not to learn that a 60-year-old hernia patient had a broken arm at age 10, but the substantial privacy protection for the patient comes from good privacy practices by the insurer, not withholding irrelevant information. If "minimum necessary" requirements mean additional paperwork, they are essentially all cost and no benefit.

De-Identified Information

Defines de-identified information as information from which 18 specified types of identifiers have been removed, or information for which an expert determines that the risk of identification is very small. De-identified information is not subject to the rule. Disclosure of a code or other means of enabling de-identified information to be re-identified constitutes disclosure of protected health information. [164.502(d); 164.514(a)-(c)]

The concept of "de-identified information" will be a playground for regulators. Future research will certainly turn up new strains of identifiers and variations on old strains. Each one will have to be stamped out in order for information to earn or retain the vaunted status of "de-identified." A cottage industry of "de-identification experts" can not be far off.

This bureaucratese compares unfavorably to the privacy protection regime offered by the state privacy torts. The torts say to health care providers (and indeed everyone): "Do what you will with information provided you do not invade privacy." It is left up to providers to risk legal liability and damage to reputation if they fail to protect privacy for any reason, including failure to mask patients' identifying information from the public.

Payment, Treatment, and Health Care Operations

Health care providers must obtain a patient's one-time consent in writing before using or disclosing health information for treatment, payment, or other routine health care operations. Providers may condition treatment on obtaining such consent. (Health plans and clearinghouses may also obtain consent for their own use and disclosure of health information for treatment, payment, or other routine health care operations, and may condition enrollment on obtaining such consent.) Patients have the right to request restrictions on these types of use and disclosure, but covered entities are not required to agree to such a request. Patients may revoke their consent at any time. [164.506; 164.522(a)]

The requirement for providers to obtain an individual's prior written consent to use or disclose protected health information for treatment, payment or health care operations was eliminated. The August 2002 rule permits covered entities to obtain consent, but does not require it. Although patient authorizations will still be required to use and disclose information for purposes outside of treatment, payment, and health care operations, the August 2002 rule standardizes the core requirements in authorization forms, and allows health care groups to use a single type of authorization to get permission to use information for a specific purpose or disclosure.

The August 2002 rule explicitly permits incidental disclosures resulting from activities such as discussions at nursing stations, the use of sign-in sheets, calling out names in waiting rooms, etc., provided reasonable safeguards and minimum necessary

requirements are met.

The December 2000 rule prevents a provider from disclosing protected health information to another entity for other than treatment purposes. A covered entity is permitted to disclose protected health information to other covered entities and to noncovered health care providers to enable the recipient to make or obtain payment. Protected health information may also be disclosed to another covered entity for specified operational purposes of the recipient.

Prior to the HIPAA privacy rule, health privacy was guarded by contract, among other things. Even if a patient did not sign a form consenting to disclosure, privacy-protective terms of the treatment agreement were dictated by custom and common practice. These included sharing of information as necessary to advance treatment or payment, and assurance that information would be handled discreetly and tactfully.

The regulation creates the dreadful, privacy-destructive possibility that these contractual protections for privacy will go away. This section contains detailed regulatory dictates about what information may be shared for payment, treatment, and health care operations. Other sections mandate the terms by which information may be shared for "non-routine" purposes (see *Non-Routine and Non-Health Care Disclosures* below). Still other sections allow sharing to happen without the patient's authorization (see *Disclosures Not Requiring Authorization* below). The HIPAA privacy regulation creates the real likelihood that the implied privacy contract in health care services is going away, replaced by a uniform national regulatory regime.

In the context of payment, treatment, and operations, the December 2000 rule aped the contract-forming process by giving patients a form to sign and the opportunity to request restrictions. But the August 2002 rule took the form-signing requirement away, making it seem more likely that contractual protections for privacy will not survive the regulation.

By encouraging the conversion of privacy protection from a contract basis to regulation, the HIPAA privacy rule has dramatically disempowered consumers. Health privacy decisions have been moved further away from consumers, rather than closer to them. A patient who wants special treatment for his or her information will have a harder time getting custom service because the regulatory dictates have high civil and criminal penalties.

Rather than solving the privacy problems in our monolithic and bureaucratic health care system, privacy decisions have been moved to the most monolithic and bureaucratic system of all — the federal government. It is fair to conclude that the HIPAA privacy rule presents a step backward for true, consumer-oriented privacy protection.

Directory Assistance and Next of Kin

Requires covered entities to give patients notice and the opportunity to opt out before information is disclosed to a facility director or provided to next of kin or other persons involved in the patients' care. [164.510]

Oh good — another form for patients to fill out.

Non-Routine and Non-Health Care Disclosures

Covered entities must obtain a patient's specific authorization in writing before using or disclosing health information for non-routine uses and most non-health care purposes (see *Disclosures Not Requiring Authorization* below). Covered entities may not condition services or payment on receipt of such authorization. Patients may revoke their authorization at any time. [164.508]

Like the section on payment, treatment, and health care operations in the December 2000 rule, this section apes the contract-forming process by giving patients a form to sign. In fact, the resulting "right" to refuse information-sharing may be regulatory rather than contractual. With almost no individual power to enforce a regulatory "right" (see *Enforcement* below), consumers are not better off under the regulation than they were before it existed.

Business Associates

Allows a covered entity to disclose health information to a business associate without further authorization if it obtains satisfactory assurances, through a written contract, that the business associate will safeguard information. The contract must establish the permitted and required uses and disclosures of such information by the business associate. A business associate may use health information for its own management and administration, and may disclose it to others if it obtains assurances that the information will be held in confidence and the recipient will notify the business associate of breaches of confidentiality. [164.502(e); 164.504(e)]

The August 2002 rule allows covered entities, except small health plans, up to one year beyond the April 14, 2003 enforcement date to change existing contracts with business associates.

The "business associates" provisions have been the product of much hand-wringing, but business associates have probably always been under at least implied contractual obligations to use information in ways that do not invade privacy. Business associates of health care providers, like all private entities that hold sensitive personal information, are obliged by the privacy torts to deal with that information using tact and sensitivity.

Employers

Employers that sponsor health plans may not obtain and use employees' health information for employment or other non-health purposes without their specific authorization. [164.504(f)]

Employers are driven into the provision of health care by poor tax policy that does not give individuals parallel tax benefits for buying their own insurance. Fixing that problem would help restore privacy and do much more to benefit American patients.

Hybrid Entities

Requires hybrid entitites (i.e., companies with multiple lines of business) to restrict disclosure of health information between their health care and non-health-care components. Such disclosures are governed by the same restrictions as disclosures between two separate and distinct legal entities. [164.504(b)(c)]

Those dang hybrid entities were the problem all along.

Disclosures Not Requiring Authorization

Covered entities may use and disclose health information without a patient's authorization for the following national priority activities, consistent with other applicable laws and regulations: (a) uses and disclosures required by law; (b) public health activities; (c) abuse, neglect, and domestic violence; (d) health oversight; (e) judicial and administrative proceedings; (f) law enforcement; (g) coroners, medical examiners, and funeral directors; (h) organ donation and transplantation; (i) research; (j) imminent and serious threats to health and safety; (k) specialized government functions; (l) workers' compensation programs. [164.512]

The December 2000 privacy rule provides that protected health information may not be used or disclosed for research without either a written authorization or a waiver of authorization approved by the Institutional Review Board or a Privacy Board. In the August 2002 rule, HHS significantly simplified the administrative burdens for obtaining authorizations and assessing requests for waivers of authorization.

This section squarely deprives American patients of power to control information about themselves. Needless to say, many of the reasons for sharing information found in this section are good policy or appropriately required by the legal system. But participation in research and "public health activities" will no longer be a matter of choice to be approved by good citizens. The health care arena is likely to operate on the assumption that the full range of federally approved disclosures is approved by patients.

Because information may be disclosed for governmental "health oversight," doctors will be fearful of liability if they do not retain records for those purposes. Truly confidential medical treatment — treatment about which the doctor disposes of his or her records — has been laid to waste by the HIPAA privacy rule.

Marketing and Fundraising

Covered entities may use or disclose information without a patient's authorization to market their own products or services, or the products or services of others, as part of the treatment of that individual. Covered entities must identify themselves when making a marketing appeal and give patients the opportunity to opt out of any further communications. Covered entities also may disclose certain patient information to a foundation or business associate that contacts patients for fundraising purposes, provided that patients are given the opportunity to opt out of any further communications. [164.514(e)(f)]

The August 2002 rule requires covered entities to obtain prior patient authorization for marketing, except for face-to-face communication or a communication involving a promotional gift of nominal value. The rule distinguishes between activities that are and are not marketing. The definition of "marketing" in the new rules excludes communications by a health care provider promoting its own goods and services.

Treating unwanted marketing as a "privacy" problem is a favorite pastime of anti-commercial privacy activists because it blends their distrust of corporations with an issue that few people can second-guess them on. A good deal of marketing is premised on sellers knowing little or nothing about consumers but presuming to contact them anyway. This is hard to square with the heart of the privacy problem, which is too much information available too widely.

There are genuine concerns about marketing of health care products and services, but they are more complex than people think. For example, if adult diapers are marketed to a person suffering from incontinence, an obvious inference is that his or her private health information has been revealed to someone (even if it has only been computers and machines). But if adult diapers are marketed to everyone over 65, some recipients of the advertising may still feel that private information has been revealed when it has not. Others would learn for the first time of a sanitary option that gives them more freedom to go out in public.

Marketing of health care products and services carries risks to privacy and perceptions of privacy. But it also can inform the public of cost-savings and new treatments that improve and extend life.

Psychotherapy Notes

Provides higher level of protection than for other types of health information. Requires authorization for most uses or disclosures. Health plans may not condition enrollment or eligibility for benefits on obtaining such authorization. [164.508(a)(2)]

As if the treatment community was not aware of the stigma that sometimes attaches to mental health services . . . .

Preemption of State Laws

Preempts all contrary state laws unless they are more stringent (i.e., more protective of privacy). Does not preempt state parental notification laws or state laws used to administer health care, regulate controlled substances, or protect public health, safety and welfare. Allows states to apply to HHS for a determination on whether a state law meets the requirements of these exclusions. [160.201 *et seq*.]

The December 2000 privacy rule generally gives control of health information about a minor to the parent, guardian, or person acting in loco parentis. The August 2002 rule clarifies that state law governs in the area of parents and minors, and that HIPAA does not overturn state laws that give providers discretion to disclose or deny health information to parents.

The preemption portion of the HIPAA privacy regulation pulled off an incredible feat by leaving in place state law that is more protective of privacy *without identifying what privacy is*. In truth, the regulation leaves the Department of Health and Human Services with total discretion to find state law preempted or not preempted depending on what concept of privacy the Department adopts from time to time. Until HHS rules, lawyers and judges will wrestle with the problem and consumers will not know what the law on privacy may be.

Perhaps, because people so often protect privacy by contract, the preemption provision preserves contract law so that consumers can reject the disclosures found in the *Disclosures Not Requiring Authorization* section of the HIPAA privacy regulation. But just as often, consumers contract away privacy of information in favor of lower prices, tailored products, good customer service, and so on. If the preemption section means what it says — whatever that is — patients may still require by contract that information about them is used for the purposes they want.

Safeguards

Requires covered entities to establish and implement various administrative procedures, commensurate with the size and scope of their business, to protect the confidentiality of health information. These include designating a privacy officer, training employees, and developing a system of sanctions for employees who violate an entity's privacy policies. [164.530]

This is yet another regulatory playground. Rather than focusing on when consumers' privacy is protected and when it is not, bureaucrats can study health care business processes and demand changes from time to time based on fads like the "Chief Privacy

Officer." A cottage industry of government-approved privacy consultants and trainers will undoubtedly feed at this trough.

Compliance

Permits an individual, who believes a covered entity is not compliant, to file a written complaint with the Secretary. Authorizes Secretary to conduct a compliance review of such an entity. [160.300 *et seq*.]

"This time, I am going to write a *very* angry letter to the Secretary of Health and Human Services!"

Enforcement

HIPAA imposes civil monetary penalties against covered entities that fail to comply with the rule and imposes criminal penalties for certain wrongful disclosures of health information. Civil fines are $100 per person for unintentional disclosures, capped at $25,000 per year. Criminal penalties for selling, transferring, or using health information for commercial advantage, personal gain, or malicious harm include fines up to $250,000 and/or up to 10 years in prison. [42 U.S.C. 1320d-5,6]

Enforcement is the key area where regulation fails consumers compared to contracts and tort law.

If a health system shares information contrary to a patient's wishes in the contract environment, the patient can sue for violation of the contract and recover damages. If the right to refuse information sharing comes only from the HIPAA privacy regulation, the consumer can only complain to the Department of Health and Human Services, getting in line behind thousands of other people to see if the agency will pursue his or her interests. In the regulatory setting, enforcement depends on who has good lobbyists and good luck. It can be sporadic, politically motivated, or hyper-technical, depending on which way the winds are blowing in Washington, D.C. Businesses that keep lobbyists on staff and on retainer generally have better luck than individual consumers seeking justice for themselves.

The solution is not to create private causes of action for regulatory violations. This would just invite a parade of class action lawyers to sue over paperwork violations. Rather, our policy should focus on making whole people who suffer real harms. The private causes of action found in contract and tort law do precisely this.