THE HIPAA PARADOX

The Privacy Rule That's Not

by Richard Sobel

HIPAA is often described as a privacy rule. It is not. In fact, HIPAA is a disclosure regulation, and it has effectively dismantled the longstanding moral and legal tradition of patient confidentiality. By permitting broad and easy dissemination of patients' medical information, with no audit trails for most disclosures, it has undermined both medical ethics and the effectiveness of medical care.

Most physicians, patients, policy analysts, and journalists believe that the HIPAA "privacy rule" protects medical confidentiality. They are mostly incorrect. The Health Insurance Portability and Accountability Act creates medical records rules that tighten internal practices, like hiding computer screens and not talking in elevators, and these protections are an improvement over previous practice, but they are limited.[1] Perhaps because the enabling legislation called for a "standard for privacy of individually identifiable health information" and the original final rule in 2000 required patient informational consent, there is a belief that the Department of Health and Human Services rules provide strong privacy protections for medical information. Unfortunately, that belief is a misconception.[2] In fact, the amended final HIPAA rule (for simplicity, hereafter referred to as "HIPAA," or "the HIPAA rule") provides much less privacy than the term "privacy rule" suggests.

Rather than broadly protecting privacy, the amended HIPAA rule generally constitutes a *disclosure* regulation.[3] As first issued in August 2002,[4] the HIPAA rule specified how health information may be used and disclosed, and it only partly keeps medical records confidential. Effective in April 2003, the federal government gave six hundred thousand "covered entities"—such as health care plans, clearing-

Richard Sobel, "The HIPAA Paradox: The Privacy Rule That's Not," *Hastings Center Report* 37, no. 4 (2007): 40-50.

houses, and health maintenance organizations—"regulatory permission to use or disclose protected health information for treatment, payment, and health care operations" (known as TPO) without patient consent.[5] Some of these "routine purposes" for which disclosures are permitted are far removed from treatment. In fact, "covered entities" and their "business associates" may share patients' sensitive personal information for treatment, payment, and health care operations without the patients' knowledge, over their opposition, and even if patients pay for treatment out of pocket or request the right to be asked for consent to disclosure of their medical records.[6]

Particularly troubling is the governmental authorization for covered entities to use patients' confidential health information without their consent for health care operations

HIPAA Rules and Challenges: A Timeline

Health Insurance Portability and Accountability Act, Pub. L. 104-191, 110 Stat. 1936, especially Title II, Subtitle F (administrative simplification), Secs. 261-4; 42 USC Secs. 1320d-d8; 45 CFR Secs. 160-164, especially 164.506-512	August 21, 1996
Authority for privacy rule delegated to DHHS secretary	August 21, 1999
Proposed original rule (without a consent requirement), 64 *Federal Register* 59,918 (Notice of Proposed Rule-Making and Order 1999)	November 3, 1999
Comment period	November 3, 1999, to January 3, 2000, extended to February 17, 2000
Original rule (final, with consent), 65 *Federal Register* 82,462, 45 CFR 160, 164, esp. 506(a)	December 28, 2000
Additional comment period, 66 *Federal Register* 12,738 (Notice of Proposed Rule-Making and Order 2001)	February 28, 2001, to March 30, 2001
Original rule effective date (with consent), 66 *Federal Register* 12,434	April 14, 2001
Proposed amended rule (without consent), 67 *Federal Register* 14,776 (Notice of Proposed Rule-Making and Order 2002)	March 27, 2002
Additional comment period	March 27, 2002, to April 26, 2002
Amended rule (final, without consent), 67 *Federal Register* 53,182, 45 CRF 160, 164 (2002)	August 14, 2002
Amended privacy rule effective date, 67 *Federal Register* 53,182	October 15, 2002
Compliance date (for large entities; small health plans given an additional year)	April 14, 2003 (originally February 26, 2003)
Citizens for Health et al. v. Thompson filed	April 10, 2003
District Court Decision, Judge Mary A. McLaughlin, Philadelphia, 03-2267	April 2, 2004
Appellate Court Decision, *Citizens*, 428 F. 3rd 167	October 31, 2005
U.S. Supreme Court cert. petition, *Citizens*, cert. denied, 127 S. Ct. 43	October 3, 2006

that are unrelated to payment or treatment. "Health care operations" (HCO) include most administrative and profit-generating activities, such as auditing, data analyses for plan sponsors, training of nonhealth care professionals, general administrative activities, business planning and development, cost management, payment methods improvement, premium rating, underwriting, and asset sales—all unrelated to direct patient care.[7] Health care operations also include some marketing (which otherwise requires a signed authorization) and fundraising for the covered entity.[8] As distinguished from "core" treatment and "routine" payment purposes, health care operations permit the legal disclosure of information that could be inappropriately used for purposes that patients might not approve, and thereby may lead to consequences patients might not like.

In addition, covered entities may share patient information with millions of contracted "business associates" without patients' consent. Like covered entities, their business associates are supposed to keep patient information confidential.[9] But because amended HIPAA rules permit broad uses under health care operations and do not require an audit trail for "routine" disclosures, there is no way to monitor whether health information is shared in ways inconsistent with contractual requirements or patients' wishes. Thus, if patients have problems with employment or insurance because of unauthorized disclosure of their health information, the patient cannot trace the harm to a disclosure authorized under health care operations.

The Possible Harm

Confidentiality is at the heart of the doctor-patient relationship, and consent is an essential means by which patients can assure that information remains confidential.[10] There is a great need for such assurance because any problem that *could* arise with health disclosures probably will. As Ted Cooper of Kaiser Permanente noted in 2000 when he recommended that HIPAA be "crafted from the perspective of how we would want" our family's health data handled, "every permutation that can happen will happen."[11] According to health attorney James Pyles, "information such as a name and diagnostic code . . . could be enough to derail your prospects for a loan or a job. You could be charged higher loan rates or lose a job because of what's in your medical record . . . And it will be impossible to prove it was because your data was shared . . . because there is no disclosure or audit" trail under HIPAA.[12] Because of the lack of limitations, potentially harmful information is likely to be shared in the course of basic health care operations, and HIPAA actually facilitates that sharing, without patient authorization, even if other laws might prohibit the use of the information.

Pyles's comments suggest two examples of possible harm through routine disclosures under HIPAA. When sharing health information during health care operations, HIPAA could permit an insurer to give data to a bank it owns, which might then deny someone a loan on the basis of those data.[13] A cancer drug prescription from a pharmacy bought by a conglomerate that owns a mortgage company could provide the basis for deciding that a patient who may have a terminal illness is a bad lending risk, for example. While some laws protect against the disclosure of special kinds of information, such as HIV status, the lack of a HIPAA audit trail on routine disclosures means that HIPAA tends to undercut these restrictions.

Health information transmitted under HIPAA health care operations rules might also affect job prospects. HIPAA prohibits covered entities from disclosing health information for job-related purposes unless an individual signs an authorization. But an employer is not considered a covered entity unless it self-insures its health plan, so if the employer is not self-insured, it is exempt from these rules. In addition, even in those cases in which the employer is subject to these rules, the lack of audit records means the prohibition may not be enforceable. For instance, despite the HIPAA requirement for a patient's written authorization before medical records can be used for employment purposes, HIPAA lets self-insured employers receive employee health data for utilization review. Thus, a self-insured employer might legally obtain information from a physical exam on an employee without his or her authorization that reveals the employee is diabetic. The employer might then deny that person a promotion to the head of food services. Or a corporation considering acquiring a pharmacy group could view member records as part of due diligence, learn that one of its executives uses an anxiety medication, and decide she is not a good candidate for chief financial officer. As businesses learn that health information may be obtained legally through health care operations provisions without asking for authorization, the likelihood of breaches may increase.

A recent case in California shows concretely how HIPAA rules may lead to insurance or job loss. Through HIPAA procedures permitting—but not requiring—that therapy notes be kept separate, a Stanford hospital's disclosure of a patient's psychiatric records contributed to her losing a disability complaint. Because HIPAA does not require that psychiatric notes be maintained separately from other medical records, the patient's therapy information, scanned and electronically stored in the hospital's computer system with the rest of her medical records, was released to the disability insurer against the patient's wishes—and despite assurances by her psychotherapist that the notes were being kept separately and would not be disclosed without her consent. The released information contributed to a denial of disability insurance benefits for an unrelated automobile accident, then to disability discrimination

when she returned to work, and eventually to the loss of her job.[14]

Misconceptions about Protection

Medical ethics dating back to the Hippocratic Oath require confidentiality, and the pre-HIPAA practice was almost entirely to ask for patient consent to disclose information.[15] Further, some state laws and professional codes of ethics incorporated into state licensing laws explicitly require confidentiality and consent to disclose. Nonetheless, many citizens are not currently so protected. Most notices of privacy practices (also known as NPPs)—the forms handed out at doctors' offices that are supposed to explain HIPAA's rules—are written as if only the federal requirements (or their deficiencies) apply to medical information. This is so even though HIPAA's rules require that they incorporate any more stringent standards that may be set out in state laws.[16] As two physicians note, "in effect the Hippocratic Oath—the foundation of medical ethics and the most important of all patients' rights—has been rescinded by federal decree."[17] Under HIPAA, physicians neither need to nor are able to keep patient information private. Moreover, the absence of a requirement for obtaining patient consent indirectly lowers the observance of ethical and professional standards. Justice Brandeis called the government the "omnipresent teacher" for good or ill;[18] the governmental lesson here is that patient privacy need not be legally or ethically protected any more.

Ironically, providers' misunderstanding of HIPAA may generate more privacy protection than the law's actual provisions. The 2002 American Medical Association book on HIPAA says the rule requires "an initial consent to the provider's use or disclosure of PHI [personal health information] for the purposes of treatment, payment and health care operations." Although it mentions that a "proposed modification would eliminate the need for the initial consent,"[19] physicians who read this passage when consent was still part of the original final rule might not realize that the requirement has been amended away. Many physicians may yet think mistakenly that HIPAA requires patient consent for using information and thus request it of their patients.[20] But consent is now optional under the amended rule.

Similarly, administrators may believe that a HIPAA requirement for sharing only the "minimum necessary information" for insurance purposes may be generalized to all purposes, including treatment. In fact, medical providers are exempt from minimally tailoring treatment disclosures. While some doctors may still offer or ask for consent as they traditionally have—whether for ethical reasons or because they do not understand that it is now optional—most HIPAA notices do not offer the patient a chance to give consent. As more providers, patients, and policy analysts recognize that HIPAA now lacks a patient consent provision, many will realize something is seriously awry with the "privacy rule."

The notices of privacy practices that patients receive at initial clinical encounters contribute to the confusion. While the forms are supposed to tell patients what rights they have (such as seeing their records) and what rights they lack (such as consenting or withholding consent for use and disclosure), the language is complex, and many patients (and providers) misread the notices as consent forms. Patients are asked and sometimes required to sign the forms, just as they are with consent forms, and this similarity of process may itself confuse patients. But notices of privacy practices are not consent forms, and patients may or may not sign them—in fact, whether patients sign them has no effect on what happens to their medical information.[21] Oddly—and disturbingly—they are one of the main features that the DHHS identifies as protecting privacy: the DHHS asserts that they have this effect because they are supposed to encourage physicians and patients to discuss informational privacy.

In fact, under HIPAA, patients cannot prevent their information from being shared by refusing to provide their signatures or otherwise trying to withhold consent. At most, a covered entity will agree to a patient's request to be asked for his or her consent. Up to 90 percent of providers offered consent prior to HIPAA,[22] and a few providers may still ask patients for consent, but most providers do not currently offer the option on their own for the few patients who might request it. With so few providers offering them, patients cannot secure consent options by moving to another doctor.

Indeed, there are strong incentives for providers not to offer consent. Quite simply, it is easier not to. Moreover, the license HIPAA gives to covered entities with "regulatory permission" to use and disclose patient data without consent is a strong encouragement not to seek it. In addition, providers who offer a consent option incur legal liabilities of civil and criminal penalties if consent is then not obtained or the privacy promise is violated.[23] In an Orwellian reversal, not offering the consent op-

Ironically, providers' misunderstanding of HIPAA may generate more privacy protection than the law's actual provisions.

tion creates no such obligation. Not requiring providers to request consent means that those few patients who might want to withhold it to protect or negotiate for their privacy lack the right and leverage to do so.

Consent is essential to good medical care because the opportunity to offer or withhold consent provides patients with a sense of efficacy and the basic elements of control in receiving medical care. Commentators sometimes dismiss consent as a useless privacy protection. However, the problem is typically not with consent per se, but with the way it is presented. If it is forced, or if it is a merely pro forma option, then it accomplishes little. The challenge is to make the consent decision and process an integral part of all treatment and informational relationships.[24]

When patient consent was required in the original final rule, covered entities could refuse treatment, except in emergencies, to patients who declined to sign a consent form. Now, if patients refuse to sign the "privacy notice," they can still get treatment. However, some health plans may mistakenly refuse to treat those declining to sign,[25] or they may set up computer procedures that require HIPAA acknowledgement before being able to sign in. Although signing the privacy notice is without legal consequence, providers who mistakenly withhold treatment from patients who do not sign it undermine a major purpose of HIPAA—namely, to facilitate patient care.

Physicians' Concerns about Medical Privacy

National surveys show that both doctors and patients question HIPAA's benefits for medical privacy. Doctors, in particular, recognize problems with the HIPAA rule. According to a survey conducted in 2005 by Julia Slutsman and colleagues, "Most physicians . . . believe that the privacy rule does not improve the protection of confidential health information."[26] While most physicians felt that some HIPAA provisions would "somewhat or greatly" "improve privacy protections," the majority did not think either the notice provision (64.2 percent) or privacy officers (60.3 percent) would improve protection of health information.[27] Although one quarter felt that a violation of medical records privacy was a "very serious problem," less than a quarter (22.8 percent) agreed that the privacy rule would help them "maintain the confidentiality of patients' medical records." In fact, nearly half (45.4 percent) disagreed.

Two-thirds of physicians reported that written patient authorization for "nonroutine" uses of confidential patient information (other than in "treatment, payment, and health care operations") will "greatly" or "somewhat" improve privacy protection. In fact, the HIPAA requirements for a written authorization for uses in marketing, employment, or insurance give patients the control that the traditional practice of requesting consent provides. The authors found these results "contradictory." Most physicians believe that the privacy rule does not improve the protection of confidential health information, yet many feel specific requirements will improve privacy protection. What is going on here?

Physicians' perception that the privacy rule will not greatly improve privacy protections may stem partly from a belief that their "ethical and professional obligations, not regulatory mandates, assure patients' privacy and confidentiality."[28] Indeed, because the final HIPAA rule was amended in 2002 to remove patients' right to consent, only the ethical responsibilities of conscientious physicians and some state laws may keep patient information confidential. On the other hand, physicians' ethics will be severely tested when they want to promise confidentiality, but their employers, regulatory bodies, or insurers insist on access to patients' health data. In short, physicians can neither readily adhere to professional ethics nor promise confidentiality to their patients. More physicians will essentially have to offer not promises of confidentiality, but warnings, a la *Tarasoff* or *Miranda*, that what patients tell their doctors "may be used against them."[29]

Patients' Concerns about Medical Privacy

How concerned are patients about their medical privacy? And how many have had their medical information accessed inappropriately and have suffered because of it? Also, how many people are so concerned about threats to their medical privacy that they forgo medical treatment? As the Supreme Court noted in *Jaffe v. Redmond*, concern and suspicion about the possibility of losing confidentiality, especially for mental health care, can deter patients from sharing information with providers—or even seeking care in the first place—as effectively as actual breaches. As more people become aware that they do not control their medical information under HIPAA, the number avoiding treatment is likely to grow.

Public opinion surveys since the 1990s have found high levels of concern about medical privacy. In a 1993 Harris poll, 85 percent believed protecting the confidentiality of medical records was either "absolutely essential" or very important in any health care reform. In a 1994 Wirthlin survey, 83 percent of the public held that "any provider," including "a doctor," should need patient approval to send to an outside organization any diagnosis or treatment information. A 2002 Johns Hopkins University study found that 85 percent of respondents opposed employer access to genetic information.[30] In short, the public thinks their own physicians need patient approval to use their medical records, even for treatment.

A 1999 California HealthCare Foundation (CHCF) study found that one in seven patients (15 percent nationally) was taking at least one of six possible measures to hide information from their providers, including

going to different doctors or paying out of pocket.[31] A 2005 follow-up that asked only four of those six questions found one in eight patients (13 percent on average) were practicing "privacy-protective behaviors."[32] If all six questions had been repeated, about 20 percent to 22 percent would have indicated that they pursued privacy protective behaviors.[33] In short, the proportion acting on their concerns about the loss of medical privacy has grown significantly in half a decade.

The Magnitude of the Harm

While about one third of respondents (36 percent) in the 1999 CHCF study were concerned that health claims information provided to insurers might be used by employers "to limit job opportunities," the 2005 percentage rose to over half (52 percent).[34] The 1999 CHCF study found that 17 percent had experienced a breach of their health privacy—6 percent by a hospital or clinic, and 6 percent by an employer. The 2005 survey shows that one quarter of respondents (23.5 to 28 percent) "are aware of . . . specific incidents where the privacy of people's personal information was compromised."

The national CHCF surveys indicate that about a tenth had their hospitals or employers share information inappropriately. Some feel they have lost a job or insurance because of these breaches. These CHCF figures provide evidence that a significant number of patients are changing their treatment behavior because of concerns that their health privacy is not protected. Though the DHHS Office for Civil Rights has received twenty three thousand complaints about privacy violations[35]—including 5,648 in just the first year of its operation (2003-2004)—most have been dismissed for being outside HIPAA rules.[36]

Privacy protections are needed because confidentiality is essential for patients to safely share their health information with physicians who keep medical records on an electronic system. As more patients (and doctors) discover that they have no right under the HIPAA rules to give or withhold consent in controlling their health information, the proportion not providing full medical details will increase. If the problem gets bad enough that physicians are forced to diagnose without full patient information and to practice more defensive medicine, then medical mistakes and health care costs will rise. Physicians who share patients' concern about privacy may also omit information from patient records. Further, physicians may feel driven to substitute costly diagnostic testing to identify information that patients would freely share if they felt their privacy would be protected. There are few clearer examples of the information processing cliché, "garbage in, garbage out," than an electronic health system that is based on incomplete or censored patient data.

> A 1999 study found that one in seven patients was taking measures to hide information from their providers, including going to different doctors or paying out of pocket.

Problems Doctors Face

Physicians have increasing difficulty maintaining patient confidentiality under the HIPAA rules. Three non-HIPAA cases point to the problems that patients and providers face when health information is not protected by patients' right to consent under state or national law. In 1999, Dr. Sheila Horn was fired after refusing to share confidential patient information with her employer, The New York Times Company, even though her state medical society indicated she had an ethical obligation to her patients not to do so. A New York appellate court decided in her favor that she was required to follow medical ethics of confidentiality, but the State Supreme Court ruled that as an employee she could still be fired at will. (The New York Times Company had said she was released after a restructuring of its medical department.)[37]

Another case of compromised confidentiality concerns Harold Eist, a psychiatrist in Maryland, whose confidential patient records have been repeatedly demanded by the Maryland State Board of Physicians in response to a third-party complaint despite the adamant opposition of the patient, a peer review that found the third-party allegations against Dr. Eist without merit, and four court decisions supporting Dr. Eist's position in defense of medical privacy.[38] The board still maintains that it can compel Dr. Eist to disclose the patient's entire medical record and that Dr. Eist should be punished for his lack of speedy cooperation.

Even Dr. Daniel Shrager's successful protection of patient privacy reveals the pressures on physicians to share confidential patient data.[39] In this situation, Magellan Behavioral Health threatened to remove Shrager from its provider panel if he did not turn over confidential psychiatric patient data. Shrager won, although HIPAA rules permit sharing patient information with oversight and paneling agencies that demand medical records. At the very least, the case shows that physicians' careers and patients' health secrets are increasingly at

risk, and that defending them is costly.

Moreover, the official evaluations of the HIPAA rule miss the threats that providers, patients, and their records face. For example, a Government Accountability Office report in 2004 concluded that implementation of the privacy rule has not hindered the provision of health care.[40] Also in 2004, the DHHS Office for Civil Rights found that, of three thousand complaints about privacy violation lodged under HIPAA, only 259 were valid, and it levied no fines. More than a third (35.3 percent) of the complaints alleged violations that the Office for Civil Rights held were "not prohibited by the Privacy Rule," such as lack of a consent provision for use of confidential information.

In fact, in addition to the DHHS Office of Civil Rights finding that the denial of patient consent is not an appropriate criterion for complaints, the Department of Justice ruled that employees who violate the "privacy" rule do not implicate the covered entity if the individuals are not acting in official capacities. For instance, in 2004, a Seattle hospital employee who stole patient information to obtain fraudulent credit cards and goods was sentenced to sixteen months in prison. The Justice Department, however, ruled that criminal penalties only "apply to insurers, doctors, hospitals and other providers—but not necessarily their employees or outsiders who steal personal health data."[41] In short, the law does not necessarily cover the misdeeds of people who work for a covered entity because only covered entities themselves can be prosecuted under HIPAA.

Both the GAO report and the Justice Department interpretations ignore the numerous complaints about the lack of consent in the HIPAA regulations. In a medical catch-22, breaches of confidentiality from lack of consent are not breaches of HIPAA, and hence are not violations. The traditional confidentiality of doctors' and patients' relationships now survives mostly on the strength of ethical norms and misperceptions about the law. The reality is that physicians cannot promise confidentiality, and patients are unable to consent or withhold permission for use of their confidential health information. Nor can patients complain effectively when they discover that their wishes are ignored. Patients' most important concerns—about having some say in the use of their records—are neither part of the HIPAA rules nor subject to investigation by the Office for Civil Rights. In effect, HIPAA functions as a Trojan horse in breaching the edifice of medical confidentiality: it erodes ethics and lulls doctors and patients into thinking they have privacy protections.

Actual protections are increasingly limited, as this comment from an American Hospital Association spokesman revealed: "our national healthcare system can no longer beguile itself with the myth that quality care involves only one doctor and one patient alone in a room where confessions are made and promises are kept. . . . A visit to a physician may be the point of entry into the system for a given episode of illness, but it contorts the process and potentially undermines the quality of care to pretend that an institution can be reduced to a personification of the secret-protecting family doctor."[42] Similarly, the Justice Department wrote in a 2004 brief: "there is no federal common law" protecting "physician-patient privilege," and in modern medical practice, "[I]ndividuals no longer possess a reasonable expectation that their histories will remain completely confidential."[43] If there is any hope to be found, it is that this detrimental state of affairs will give patients, doctors, and policy-makers an impetus to push for improvement in privacy protections.

On the one hand, patients may refuse to disclose important but embarrassing information because their providers cannot guarantee privacy. On the other hand, physicians may have to require more tests, or play cat and mouse with patients to get more information. Some providers may simply ask less and instead try to figure out histories and diagnoses by inference.[44] Providers may also omit or mislabel information in patients' records.

The ethics and effectiveness of medical care are at risk. As physicians and patients learn that they are losing their autonomy, their control over their relationship, and the confidentiality of their most private information, ethical and practical dilemmas will abound. The tensions in the Slutsman study findings reflect physicians' recognition that HIPAA does not protect patient privacy; indeed, it weakens their ability to maintain confidence and respect professional norms.[45]

As Ascher et al. noted, the purpose of patient informational consent is "the same as the purpose behind informed consent for treatment: to show respect for patient autonomy by informing the patient of the risks and benefits, and allowing the patient to make informed decisions" about the risks and benefits of sharing health information.[46] Although some states provide more stringent laws that preempt HIPAA, the federal "privacy rule" incentives not to offer patient consent undermine traditional ethical and legal protections.

Even HIPAA Protections Could Be Diluted

One rationale for passage of HIPAA was that enacting a single, common rule for respecting the privacy of medical records would foster "administrative simplification" (45 CFR 160-164) and promote the computerization of health information. In actuality, HIPAA's lack of privacy protections undermines these efficiency goals, since if patients decide not to disclose potentially detrimental information, health care costs will rise. The transition to electronic medical records will not be successful unless respect for medical privacy is assured. Yet recent Bush administration calls to reduce health costs by pro-

moting electronic medical records still overlook this reality.[47]

Although electronic record-keeping can be valuable in preventing errors and computer systems can be made more secure by setting up multiple levels of access and permission, computers also make privacy breaches much easier and significantly more consequential. For instance, it is easier—appropriately or not—to send entire medical records at the click of a mouse than to copy and mail a large paper record. Computerization also allows sensitive information to be sent to numerous destinations as easily as to any one.

In addition, some groups are lobbying to turn what is called the HIPAA "floor" of minimal protections into a "ceiling"—setting the maximum standards—by removing patient consent requirements from stricter state laws, including those incorporating professional codes of ethics and conduct.[48] The proposed alternative would replace the state protections with provisions that facilitate "interoperable" sharing of health data without consent.[49]

For instance, the Health Information Technology Promotion Act of 2006 (H.R. 4157), a bill concerning electronic medical records that is supported by the health care industry, lacks any consent provisions. Earlier versions proposed that the DHHS secretary be authorized to remove HIPAA's preemption of more stringent state privacy laws, but that proposal has been modified. H.R. 4157 also authorizes a "National Coordinator for Health Information Technology" to set up a health surveillance databank system. The House of Representatives passed the bill in July 2006.

In the Senate, the proposed Wired for Health Care Quality Act (S. 1418) provides for the development of standards for a national, interoperable electronic medical records system. But, like its House counterpart, it does not recognize or preserve the right to health information privacy, nor does it include a provision for patient consent.

In short, even more than HIPAA, H.R. 4157 and S. 1418 would create a system in which, at the behest of covered entities, patients and providers would have virtually no health information privacy rights, and physicians would be even less able to guarantee patient privacy or to adhere to the principles of medical ethics ensuring confidentiality.

What Can Be Done?

Conscientious and cost-conscious legislators and administrators need to recognize that the price of providing privacy protections is a comparatively small part of the health care system's overall costs and is less than the expense generated by the privacy protective behavior to which patients resort when they feel their privacy is threatened. In particular, observing the ethical principle of patient consent to disclosure would be relatively inexpensive and cost effective. The American Hospital Association has estimated that only $101 million of the $22.5 billion cost of complying with HIPAA over five years[50] was attributable to asking privacy consent, as required by the original final rule.[51] In short, for less than one-half percent of HIPAA's costs, the right to consent could have been preserved,[52] so restoring the consent provisions to the HIPAA process and forms would be cost effective.

Observing the ethical principle of patient consent to disclosure, as required by the original final rule, would be relatively inexpensive and cost effective.

Besides adding a consent provision, three other changes would improve HIPAA. First, the DHHS—especially its Office for Civil Rights—and state governments should require that notices of privacy practices incorporate more stringent state laws on confidentiality and consent into their texts and protections. Second, the DHHS and its Office for Civil Rights should enforce HIPAA's provisions, including those requiring that state confidentiality laws be incorporated into notices of privacy practices. Currently, violations of HIPAA have no negative consequences.[53] Third, audit trails (especially under "health care operations") should be incorporated into HIPAA rules for uses and disclosures so that breaches can be traced.

A constitutional challenge in *Citizens for Health et al. v. Leavitt* sought to have the omission of patient consent from the amended HIPAA rule declared unconstitutional. The suit argued for recognizing protection of health privacy and patient consent to be fundamental constitutional rights, as identified in the Supreme Court's *Ferguson v. City of Charleston* decision, which stated, "the reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent."[54] *Citizens* asked the Court to find the HIPAA rule in violation of medical privacy under the Fifth Amendment right to liberty and First Amendment right to private communications by holding that HIPAA impinges on health privacy as a constitutional right. The suit's twenty plaintiffs

sought reinstatement of the original final version of the rule, which required that patients be asked for their consent. The challenge has so far been unsuccessful.[55]

There are other fronts, however. Congress should incorporate a patient consent provision into any legislation on electronic health information. Citizens can contact Congress to insist on the inclusion of privacy protections and consent provisions in bills like H.R. 4157 and S. 1418.[56] The media—especially the medical and national press—should illuminate the significance of confidentiality and consent and educate the public and leaders about the detrimental consequences of the current "privacy" rule. Powerful medical groups like the American Medical Association[57] and the American Psychological Association, acting as advocates in Congress and amici curiae in the Courts, should insist that confidentiality and consent be restored to HIPAA, both for ethical and for practical reasons.

In short, professional ethics, responsibilities, and goals mandate that medical providers and organizations support restoring patient informational consent to the HIPAA rules and electronic medical records laws. The courts and legislatures should also support patient privacy by requiring that HIPAA and electronic medical records bills incorporate the fundamental principles of medical confidentiality and patient consent into their provisions. These laws and rulings will benefit both the well-being of individual Americans and the health of the body politic by sustaining the fundamental rights to confidentiality and consent that undergird quality medical care.

Acknowledgments

Earlier versions of this article were presented for the Fellowship in the Division of Medical Ethics, Department of Social Medicine, Harvard Medical School, and at the Seminar of the Program in Psychiatry and the Law, Department of Psychiatry, Beth Israel Deaconess Medical Center, Harvard Medical School. I would like to thank colleagues in the fellowship in medical ethics at Harvard Medical School, particularly Mildred Solomon, Rick Blanks, Mary Cerreto, Stacey Ellender, Amy Farber, Stephen O'Neill, and Frank Wharam, and in the Program in Psychiatry and the Law, particularly Thomas Gutheil, Archie Brodsky, Harold Bursztajn, Michael Commons, Eric Drogin, Marc Hauser, Donald Meyer, Barry Roth, Graham Sprueill, Mitzi White, and Gary Zalkin, as well as Eric Benson, David Byrom, Heidi Kuehl, Adam Speegle, John Metz, Ole Norheim, James Pyles, Nancy Sobel, Sarah Wald, and anonymous reviewers for comments, research, and suggestions on earlier versions of this article.

Disclosure

The author and the Program in Psychiatry and the Law at Harvard Medical School were amici in *Citizens for Health et al. v. Leavitt* in the Third Circuit appeal and Supreme Court petition for writ of certiorari (www.pipatl.org/amicus.php).

References

1. The Health Insurance Portability and Accountability Act (Public Law 104-191) sets out standards for the portability of health insurance. Administrative simplification, Section 164, includes the requirements for standards on medical information—the so-called privacy rule.

2. See P. Appelbaum et al., "False Hopes and Best Data: Consent to Research and the Therapeutic Misconception," *Hastings Center Report* 27, no. 2 (1987): 20-24. The HIPAA misconception may be "therapeutic" in the sense that patients and providers mistakenly think HIPAA provides for privacy as part of the doctor-patient relationship.

3. R. Sobel, "No Privacy for All? Serious Failings in the HHS Medical Records Regulations," *Journal of Biolaw and Business* 5, no. 2 (2002): 45-48; R. Sobel, "Maintaining Informed Consent for Doctor-Patient Confidentiality: More Serious Failings in the HHS Medical Records Regulations," *Journal of Biolaw and Business* 6, no. 2 (2003): 61-65; *Citizens for Health et al. v. Leavitt*, 3rd Circuit, 428 F.3rd 167, October 31, 2005.

4. Public Law 104-191, known as the "Kennedy-Kassebaum" Bill. U.S. Department of Health and Human Services, "Standards for Individually Identifiable Health Information," 45 CFR 160-164, April 14, 2001; October 15, 2002.

5. 64 *Federal Register* 53,211, August 14, 2002, sec. 164.506a.

6. While patients may request the right to consent before the use or disclosure of their medical information (45 CFR, para. 164.552[a]), institutions do not have to agree to give the patient the opportunity to consent, and many have blanket policies refusing to do so, or refusing treatment unless the patient consents. The original final rule that included a consent provision was approved in 2000, but was amended in August 2002 to drop the consent requirement.

7. Sec. 164.501, 506. The American Medical Association has long argued against using the broad definition of health care operations. See G. Aston, "Pushed by a Looming Legislative Deadline, AMA Delegates Adopted New Policy on Patient Confidentiality Issues Tied to Participation in Medical Research," *American Medical News*, July 12, 1999.

8. The definition of marketing, which requires written patient authorization (equivalent to traditional consent), was narrowed to exclude forms of promotion such as third-party solicitations and "face-to-face communication," which therefore no longer require authorization. "Contacting of health care providers and patients with information about treatment alternatives" is also considered to be part of health care operations, and therefore does not require authorization. Some educational communications during health encounters, which could be considered marketing and hence require authorization, are defined instead as part of treatment. Fundraising under health care operations may use demographic information and dates of health care without patient consent (but with an opt-out provision afterwards) for outside organizations raising money for "the benefit of the covered entity" (164.501).

9. HIPAA creates rules for confidentiality (limitations of the range of records sharing), not privacy (patients' control of information).

10. For a discussion of the essential nature of confidentiality and consent for quality medical care, see the amicus briefs in *Citizens* and *Althaus v. Cohen* of the Program in Psychiatry and the Law at Harvard Medical School, www.pipatl.org/amicus.php.

11. M. Doscher, *HIPAA: A Short and Long Term Perspective on Health Care* (Chicago, Ill.: American Medical Association Press, 2002), 90.

12. "Eyes on Your Records," *Consumer Reports*, March 2005, http://www.consumerreports.org/cro/health-fitness/health-care/electronic-medical-records-306/eyes-on-your-record/index.htm; see also "The

New Threat to Your Medical Privacy," *Consumer Reports*, March 2006: 39 and 42. An anonymous reviewer of this paper indicated that HIPAA should not be held responsible for the violation of its provision. But by creating paths that permit misuse of information without audit trails, along with DHHS lack of enforcement and penalties, HIPAA itself arguably contributes to the likelihood that the information will be improperly used.

13. Ibid.

14. *Galvin v. Stanford Hospitals and Clinics*, California Superior Court Case No. 1-04-CV-024690, filed August 9, 2004. See Motion for Summary Judgment to Plaintiff's Second Amended Complaint, August 3, 2005; see also T. Francis, "Spread of Records Stirs Patient Fears Of Privacy Erosion," *Wall Street Journal*, December 26, 2006.

15. See also the Program in Psychiatry and the Law amicus brief, http://www.pipatl.org/amicus.php, for discussion of the conflict between HIPAA and the Nuremberg principle that "the voluntary consent of the human subject is absolutely essential." See Directive for Human Experimentation, Nuremburg Code, http://ohsr.od.nih.gov/guidelines/nuremberg.html. Some find HIPAA constitutes an unconsented experiment about the effects on patient care of unconsented disclosure of confidential medical information (see H. Bursztajn and A. Brodsky, "Captive Patients, Captive Doctors: Clinical Dilemmas and Intervention in Caring for Patients in Managed Health Care," *General Hospital Psychiatry* 21 [1999]: 239-48). For pre-HIPAA practice concerning patient consent, see 65 CFR 82771. For further details, see note 22 below.

16. 45 CFR 164.520(b)(1)(ii)(C) requires incorporating more stringent state privacy protections into notices of privacy practices.

17. B.K. Herman and D. Peel, "HIPAA's Real Effect: The End of Medical Privacy. A New Dilemma for Physician Executives," *The Physician Executive*, January/February (2004): 37.

18. *Olmstead v. United States*, 277 U.S. 438, 469 (1928) (Brandeis, J., dissenting).

19. Doscher, *HIPAA: A Short and Long Term Perspective on Health Care*, 78. See E. Redden, "Fuzzy Understandings of FERPA," June 14, 2007 at http://www.uh.edu/ednews/2007/insidehe/200706/20070614ferpa.html, on how confusion about the provisions of HIPAA and FERPA (Family Educational Rights and Privacy Act) protect privacy.

20. According to HIPAA Section 264c, the DHHS secretary "shall promulgate final regulations containing such standards"—namely, standards that set forth the privacy rights individuals should have with respect to their identifiable health information and the procedures for exercising them. The original final rule (December 28, 2000) included the following consent requirement: "(1) Except as provided . . . a covered health care provider must obtain the individual's consent . . . prior to using or disclosing protected health information to carry out treatment, payment, or health care operations." However, the similarly numbered section of the amended rule (October 15, 2002) changed this to, "The consent provisions in section 164.506 are replaced with a new provision at section 164.506(a) that provides regulatory permission for covered entities to use or disclose protected health information for treatment, payment, and health care operations."

21. The complaint in *Citizens* included twenty-five affidavits and hundreds of privacy notices issued on or after April 14, 2003, showing "that Citizens' sensitive health information was being disclosed by covered entities without notice or consent, and over their objections." Beginning April 14, 2003, under the amended rule, "virtually all covered entities switched from their practice of obtaining consent for 'routine' uses and disclosures to the unauthorized use and disclosure of health information as a result of regulatory permission in the Amended Rule." See affidavits of Deborah Peel and others; Joint Appendix to District Court Case, 238-40, 312-14, 1476-85.

22. 65 *Federal Register* 82,771. Prior to HIPAA, the DHHS estimated that "most non-hospital providers and virtually all hospitals follow this practice [of obtaining some consent for use and disclosure of individually identifiable health information]." The DHHS assumed "that 90% of the non-hospital providers and all hospitals currently obtain some consent." Yet "[w]e found among the plaintiffs in the Citizens suit that very few covered entities of any kind were obtaining consent for disclosures for treatment, payment, and health care operations after April 14, 2003. All [plaintiffs'] requests for a consent process (restrictions) were denied and large insurers like Kaiser Permanente were found to be denying all such requests." Personal communication from James Pyles, November 13, 2006. See also the affidavits cited in note 17.

23. Doscher, *HIPAA: A Short and Long Term Perspective on Health Care*, 12-13.

24. Although consent may at times be considered pro forma or granted under pressure if providers are required to seek it from patients, "coerced consent" is a contradiction in terms; it must be informed and voluntary to be meaningfully granted.

25. One patient who attempted to substitute a consent request on a HIPAA notice was denied treatment. T. Francis, "Setting the Records Straight," *Wall Street Journal*, October 21, 2006. Another wrote in an email response to the Francis article that "Every hospital and doctor I asked to 'not share my records' refused. One hospital agreed to protect the records only after I threatened to sue under Illinois Statutes after I learned that they had shared my record." Personal communication to T. Francis, October 23, 2006.

26. J. Slutsman et al., "Health Information, the HIPAA Rule, and Health Care: What Do Physicians Think?" *Health Affairs* 24, no. 3 (2005): 832-42.

27. Ibid., Exhibit 3, 838.

28. Ibid., 837.

29. *Tarasoff v. Regents of the University of California* (17 Cal. 3d 425 [1976]). See also Lamb warnings in R. Barnum et al., "Patient Warnings in Court-Ordered Evaluations of Children and Families," *Bulletin of the American Academy of Psychiatry and Law* 15, no. 3 (1987): 283-300. See also Sobel, "Maintaining Informed Consent."

30. Louis Harris & Associates, July 26, 1993, national telephone survey; Wirthlin Group, June 22, 1994, national telephone survey; Princeton Survey Research for the Genetics and Public Policy Research Center at Johns Hopkins University, October 15, 2002, national telephone survey.

31. California HealthCare Foundation, "Medical Privacy and Confidentiality Survey," 1999; http://www.chcf.org/topics/view.cfm?itemID=12500. The July 26, 1993, Harris Survey for Equifax found that 25 percent of respondents or family members had "paid for a medical test, treatment or counseling rather than submit a bill or claim under a health plan or program." The 1999 and 2005 CHCF surveys found 5 percent of individuals had paid for a medical test because they did not want an employer or others to gain access to the medical information.

32. California HealthCare Foundation, "National Consumer Health Privacy Survey 2005," 2005, 19; http://www.chcf.org/topics/view.cfm?itemID=115694.

33. Comparisons of the 1999 and 2005 CHCF surveys found that the proportion trying to hide medical information rose from 15 to over 20 percent. The 1999 survey found 3 percent nationally had asked a doctor not to write down a medical problem in their record or had gone to another doctor to avoid telling their regular doctor about a health condition, and in 2005, both figures grew to 5 percent. The 1999 figure of 15 percent engaging in privacy protecting behavior was based on six questions; the 2005 figure on only four of them. Statistical extrapolations (available from the author) estimate a comparable figure for 2005 at 20 to 22 percent. In short, the proportion engaging in privacy protecting behavior rose

by over one-third in six years. How much HIPAA's lack of privacy protections contributed to the rise can be estimated in a later study.

34. See D. Linowes, "Many Companies Fail to Protect Confidential Employee Data," University of Illinois Survey Research Lab, Fall 1995, http://www.epic.org/privacy/workplace/linowesPR.html. One-third of employers in the survey acknowledge using health information for employment decisions.

35. Francis, "Setting the Records Straight."

36. U.S. Government Accountability Office, "Health Information: First-Year Experiences under the Federal Privacy Rule," report to the chairman, Committee on Health, Education, Labor, and Pensions, U.S. Senate, GAO-04-965, September 3, 2004.

37. *Horn v. New York Times*, No. 20, 2003 NY LEXIS 221, Ct. App. February 25, 2003.

38. *Harold Eist v. Maryland State Board of Physician Quality Assurance* (Civil Case No. 240300, Cir. Ct. Montgomery County; No. 00329, Court of Special Appeals of Maryland) and 29 Brief of Amicus Curiae, including the Program in Psychiatry and the Law, October 20, 2006, in support of Eist's position. The estranged husband of a divorcing mother and children in therapy with Eist filed a complaint about the therapy with the Maryland Board, which demanded the family records.

39. *Daniel S. Shrager, M.D., v. Magellan Behavioral Health, Highmark Blue Cross and Blue Shield and Green Spring Health Services*, Allegheny County (Pa.) Common Pleas Court, Civil Division (C.D. PA, GD 00 – 015809). In deciding that a health plan wrongly terminated a psychiatrist who refused to turn over complete patient records as part of a quality improvement assessment, the court's affirmative answer reinforces the importance of the physician-patient relationship.

40. U.S. Government Accountability Office, "Health Information." The report explains, "Nearly two-thirds of the privacy complaints closed during the rule's first year of operation fell outside the scope or time frame of the rule. This included the 35.4 percent of closed privacy complaints that involved alleged actions by providers, health plans, or other entities that OCR [Office of Civil Rights] determined would not constitute violations of the regulation even if true. In other words, they concerned actions to which the patient might object, but that were not prohibited by the Privacy Rule" (p. 22, cf. Table 1).

41. R. Pear, "Ruling Limits Prosecution of People Who Violate Law on Privacy of Medical Records," *New York Times*, June 7, 2005.

42. R. Pyles, "Brave New World," *The American Psychoanalyst* 39, no. 3 (2005): 31-32, at 31.

43. T. Sloane, "It's Private When They Say So," *Modern Healthcare*, February 23, 2004, 22. Department of Justice brief, "Opposition to Northwestern's Motion to Quash Subpoena," *National Abortion Federation et al. v. Ashcroft*, No. 04 C 0055 (N.D. III).

44. See Program in Psychiatry and the Law amicus brief to Supreme Court cert. petition in *Citizens* on the costs from the absence of confidentiality and consent, pp. 10-11.

45. In addition, misunderstanding of HIPAA, which permits public health disclosures, may reduce the reporting of infection diseases; M. Wolf and C.L. Bennett, "Local Perspective of the Impact of the HIPAA Privacy Rule on Research," *Cancer* 106, no. 2 (2006): 474-79. Also, the requirement for authorizations for research may reduce research study participation; D. Armstrong, "Potential Impact of the HIPAA Privacy Rule on Data Collection in a Registry of Patients with Acute Coronary Syndrome," *Archives of Internal Medicine* 165 (2005): 1125-29.

46. J. Ascher, D. Body, and M. Leppert, "HIPAA Privacy: HIPAA Standards for Privacy of Individually Identifiable Health Information: An Introduction to the Consent Debate," *Journal of Health Law* 35, no. 3 (2002): 387; for a similar point, see the Health Privacy Project, "Comments on Proposed Modification to Federal Standards for Privacy of Individually Identifiable Health Information," April 26, 2002, 1; http://www.healthprivacy.org/usr_doc/NPRM_HPPComments.pdf.

47. M. Clyne, "President to Push Medical Record Computerization," *Baltimore Sun*, January 6, 2006.

48. See comments of the Health Care Leadership Council at the meeting of the U.S. House Ways and Means Subcommittee on Health, March 29, 2003.

49. See information on the DHHS contract with Research Triangle Institute (RTI) to identify "barriers" to interoperability of electronic medical records; http://www.mahealthdata.org/forums/hispc/index.html.

50. Doscher, *HIPAA: A Short and Long Term Perspective on Health Care*, 79.

51. The DHHS noted (65 *Federal Register* 82,771) that "for providers that currently obtain written consent, there is only a nominal cost for changing the language on the document [to ask consent]. For this activity we assumed $0.05 cost per document for revising existing consent documents."

52. Doscher, *HIPAA: A Short and Long Term Perspective on Health Care*, 79. The additional health care and other expenses created when 20 percent of patients feel required to pursue privacy-protecting behavior likely exceed the cost of consent ($101 million) by a great deal. Research is needed to establish the magnitude of the costs.

53. I draw here upon the policy suggestions of colleagues at the Program in Psychiatry and the Law, particularly Michael Commons and Barry Roth.

54. *Ferguson v. City of Charleston*, 532 US 67, 78 (2001). See also *Gruenke v. Seip*, 225 F.3rd 290 (34d Cir. 2000) and *Sterling v. Borough of Minersville*, 232 F.3rd 190, (3rd Cir. 2000).

55. See the Program in Psychiatry and the Law amicus brief in *Citizens*, available at http://www.pipatl.org/amicus.php. The district (03-02267) and appeals courts (04-2550) ruled against the plaintiffs largely on state action grounds: private entities are denying the right to medical privacy, and courts cannot force private actors to respect constitutional protections. The plaintiffs instead maintain that granting private entities the "license" of regulatory permission to use patient medical records without their consent constituted governmental action, as did levying fines for offering consent but not seeking it or violating confidentiality. The Supreme Court (05-1311, 127 S. Ct. 43) denied the petition for a writ certiorari to review the case on October 3, 2006. The plaintiffs are considering further legislative and litigation strategies.

56. Concerned patients and providers can contact the U.S. Senate Committee on Health, Education, Labor and Pensions and the House Committee on Energy and Commerce to urge them to include privacy and consent provisions in S. 1418 and H.R. 4157.

57. See American Medical Association Ethical Force Program, "The Domain of Health Care Information Privacy: Protecting Identifiable Health Care Informational Privacy: A Consensus Report on Eight Content Areas for Performance Measure Development," December 2000; www.ama-ssn.org/ama/pub/category/7726.html. The Ethical Force Program states: "Whenever feasible, health information trustees should obtain valid informed consent from individuals for the collection, storage, or use of personally identifiable health information" (p. 15). See S. Lohr, "Doctors' Journal Says Computing Is No Panacea," *New York Times*, March 9, 2005. The AMA has, however, supported electronic medical record systems that underplay privacy and consent issues; see materials available at www.ama-assn.org/ama/pub/category/16195.html.