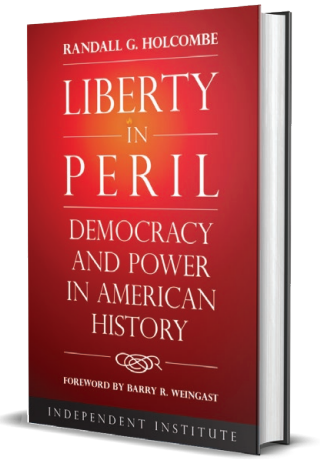
SUBSCRIBE NOW AND RECEIVE A FREE BOOK!

"***The Independent Review*** does not accept pronouncements of government officials nor the conventional wisdom at face value."
—**JOHN R. MACARTHUR**, Publisher, *Harper's*

"***The Independent Review*** is excellent."
—**GARY BECKER**, Nobel Laureate in Economic Sciences

Subscribe to ***The Independent Review*** and receive a free book of your choice such as ***Liberty in Peril: Democracy and Power in American History***, by Randall G. Holcombe.



Thought-provoking and educational, ***The Independent Review*** is blazing the way toward informed debate. This quarterly journal offers leading-edge insights on today's most critical issues in economics, healthcare, education, the environment, energy, defense, law, history, political science, philosophy, and sociology.

Student? Educator? Journalist? Business or civic leader? Engaged citizen? This journal is for YOU!

Order today for more *FREE* book options

SUBSCRIBE

The Independent Review is now available digitally on mobile devices and tablets via the Apple/Android App Stores and Magzter. Subscriptions and single issues start at $2.99. **Learn More.**

Download on the App Store | GET IT ON Google Play | Available on MAGZTER

INDEPENDENT INSTITUTE, 100 SWAN WAY, OAKLAND, CA 94621 • 1 (800) 927-8733 • ORDERS@INDEPENDENT.ORG

Health and Human Services "Privacy" Standards

The Coming Destruction of American Medical Privacy

CHARLOTTE TWIGHT

Federal privacy regulations issued by the Clinton administration on December 28, 2000, and adopted by the Bush administration on April 14, 2001, perpetrate a fraud on the American people, proclaiming privacy as their goal when ever-wider access to individual medical records is their actual and intended effect. In this article, I document the stark contrast between what Americans want and what they are getting from the federal government with respect to medical privacy, examining how and why that incongruity emerged.

Recently, the high value that ordinary Americans place on medical privacy was shown in a September 2000 Gallup poll sponsored by the Institute for Health Freedom, in which the respondents strongly opposed unauthorized access to medical records. Seventy-eight percent regarded the protection of the confidentiality of their medical records as "very important"; 91 percent opposed government-mandated medical identification numbers; and 88 percent opposed storing patient medical records in a national computerized database for use without the patient's permission. Questioned about who should be allowed to see individuals' medical records without their consent, 92 percent of the respondents opposed access by government agencies, 88 percent by law enforcers ("police or lawyers"), 95 percent by banks, 84 percent by employers, and 67 percent by medical researchers. Fully 95 percent agreed that doctors and hospitals

Charlotte Twight is a professor of economics at Boise State University.

The Independent Review, v.VI, n.4, Spring 2002, ISSN 1086-1653, Copyright © 2002, pp. 485– 511.

should be required to obtain an individual's permission before storing his medical records in a national computerized database (Gallup Organization 2000).

Ironically, unbeknown to the majority of respondents, most of the threats to medical privacy mentioned in the Gallup survey had already been either enacted into law or proposed as part of regulatory efforts to implement existing law. Yet only 16 percent of those surveyed had heard of new federal laws and regulations changing the rules regarding access to personal medical records, and 87 percent were not aware of a "federal proposal to assign medical identification numbers, similar to a social security number, to you and all other Americans to create a national database of medical records" (Gallup Organization 2000, 8, 12–13).

However, the laws were already on the books, and their implementation was accelerating. In April 2001, federal regulations adopted in the name of medical privacy further expanded access to individually identifiable medical records, without patient permission, by some of the very groups whose unauthorized access Americans most strongly oppose. How did this widely opposed result come about?

"Administrative Simplification" and the Erosion of Medical Privacy

The federal legislation underlying the new regulations is part of the Health Insurance Portability and Accountability Act (HIPAA), commonly known as the Kennedy-Kassebaum bill (Public Law 104-191, August 21, 1996). Enacted in 1996 with virtually no opposition, HIPAA seemed to foreshadow only good things—at least, it did so if one listened only to government officials and to the popular press. Members of Congress, the president, and the news media repeatedly emphasized HIPAA's appealing objectives, chief among them reduction of the "job lock" that tied many workers to their existing employment for fear of losing insurance coverage if they switched jobs.

Prior to HIPAA's passage, however, lawmakers and the press seldom told the public about the act's more ominous side—privacy-threatening provisions buried in a section entitled "Administrative Simplification," which included some of the most feared elements of the rejected 1993 Clinton health security bill. Copied almost verbatim from the 1993 bill were HIPAA's requirements for uniform electronic databases of personal medical information nationwide and for the creation of a "unique health identifier" for every American. The 1996 act empowered the federal government, at its discretion, to require detailed information on what lawmakers called "encounters" between doctors and patients. The secretary of the U.S. Department of Health and Human Services (HHS) was to adopt standards to enable "health information"—that is, everything a doctor, employer, university, or life insurer ever learns about an individual—"to be exchanged electronically." The legislation aimed to create a "health information system" through the "establishment of standards and requirements for the electronic transmission of certain health information" by medical practitioners (Public Law 104-191, Title II). The issuance of privacy regulations

to protect this new electronic flow of personally identifiable medical information was not required until three and a half years after the passage of HIPAA.[1] Yet dissent—or even attention to these provisions—scarcely arose.

In the winter 1998 issue of *The Independent Review,* I analyzed HIPAA's privacy-threatening provisions and showed that provisions related to a medical ID number and to an electronic database—along with broad new civil and criminal punishments potentially applicable to honest doctors acting in the best interest of their patients—gained passage by means of the same political tactics that had facilitated enactment of the original Medicare law in 1965 (Twight 1998). Misrepresentation, the tying of unpopular measures to popular ones, incrementalism, and other forms of political transaction-cost manipulation were as instrumental in 1996 as they had been in 1965. It was emblematic of these strategies that the electronic database and health-identifier provisions were tucked in the back of the law under the rubric "administrative simplification."

These statutory provisions have spawned an outpouring of new regulations that will soon destroy our medical privacy. The same tactics that spawned Medicare and HIPAA are being employed again in the regulatory implementation phase of HIPAA.

HIPAA Regulations: Privacy and the Standardization of Medical Records

Congress did not formulate the medical privacy standards that took effect in April 2001. Instead, it delegated that responsibility, along with other duties under HIPAA, to HHS. Between 1996 and 2000, HHS released HIPAA-based regulatory packages one by one: hundreds of pages of proposed rules, explanations of proposed rules, responses to public comments on proposed rules, preliminary releases of final rules, actual final rules, explanations of final rules, and much else. The HHS fine print fills a stack of paper already more than nine inches high and still growing, unapproachable and surely indecipherable by the average citizen. But why should ordinary people bother to read it anyway? Media and government sources continue to assert the benign nature of the new regulations, which are said to promise cost savings through database standardization along with protection of people's medical privacy. Why be concerned?

One reason for concern is that recent HHS regulations have created an architecture for the standardization of our medical records that facilitates their integration into comprehensive medical portraits of individuals. Carrying out its HIPAA mandate, HHS in August 2000 published a final rule titled "Standards for Electronic

1. "If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by the date that is 36 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than the date that is 42 months after the date of the enactment of this Act" (HIPAA, Public Law 104-191, Aug. 21, 1996, sec. 264[c]). Congress did not pass legislation establishing such privacy standards, so the task fell to HHS.

Transactions" (hereafter, the "transactions rule"), a regulatory package that specifies uniform nationwide formats and codes for electronic medical records (U.S. Dept. of HHS HCFA 2000).

Although data formats and codes may sound boring and technical, they lie at the heart of the federal government's current quest to acquire centralized medical data about us. Intended to standardize most electronic medical records nationwide, the transactions rule makes it much easier to transmit and combine medical information about an individual from diverse sources. Calling it the "most dangerous aspect of the new regulations," Representative Ron Paul (R.-Tex.), a physician, stated:

> All health care providers, including private physicians, insurance companies, and HMOs, will be forced to use a standard data format for patient records. Once standardized information is entered into a networked government database, it will be virtually impossible to prevent widespread dissemination of that information. . . . The truth is that a centralized database will make it far easier for both government agencies and private companies to access your health records. (Paul 2001)

Even HHS secretary Donna Shalala acknowledged the threat to privacy created by the transactions rule, stressing the importance of adopting privacy rules to offset it. HHS stated, "If the privacy standards are substantially delayed, or if Congress fails to adopt comprehensive and effective privacy standards that supercede [*sic*] the standards we are developing, we would seriously consider *suspending* the application of the transaction standards or taking action to withdraw this rule" (U.S. Dept. of HHS HCFA 2000, 50365; my emphasis). How often does one encounter a federal agency that, having just created a regulation, immediately expresses a willingness to suspend it?

A close reading of the transactions rule clarifies the reasons for these extraordinary expressions of concern. The transactions rule mandates nationwide use of specific, standardized *code sets* for recording medical information (*data elements*) applicable to "standard transactions." The eight identified standard transactions are:

- Health care claims or equivalent encounter information
- Eligibility for a health plan
- Referral certification and authorization
- Health care claim status
- Enrollment and disenrollment in a health plan
- Health care payment and remittance advice
- Health plan premium payments
- Coordination of benefits (U.S. Dept. of HHS HCFA 2000, 50370-72)

These categories are broadly defined. "Health care claims or equivalent encounter information," for example, include not only actual reimbursement claims but also, in the absence of any direct claim, "the transmission of encounter information for the purpose of reporting health care" (U.S. Dept. of HHS HCFA 2000, 50370, §162.1101[b]). In other words, even without a claim for reimbursement, reports of personal conversations with our physicians—deemed by the federal government to be "encounter information"—are to be treated as valid input to the ever-growing medical databases. With such a broad interpretation of the key terms, what medical transaction would not fit into at least one of the listed categories?

Records of these standard transactions must conform to the uniform data elements and code sets mandated by the new regulations. Data elements denote categories of information to be reported, and code sets establish the specific codes to be used to "fill in" a data element. Thus, the code sets establish uniform codes for items such as specific diseases, injuries, impairments, diagnoses, treatment, drugs, physician services, radiologic procedures, clinical laboratory tests, and so on (U.S. Dept. of HHS HCFA 2000 , 50370, §162.1002). For example, a health care claim transaction document might contain, as one of its data elements, the attending physician's "diagnosis." The diagnosis data element would then be filled in using one of the uniform codes covering the full range of potential diagnoses.

All *covered entities*—health plans, health care clearinghouses, and every health care provider "who transmits any health information in electronic form"—must use the standardized codes and data elements (U.S. Dept. of HHS HCFA 2000, 50365, §160.103). The number and detail of these codes and elements are astonishing. Not counting the actual codes, the basic data elements to which the codes pertain fill eleven pages, three columns per page (U.S. Dept. of HHS HCFA 1998a, 25310). These data elements include such things as patient Social Security number, claim submission and reason code, condition codes, diagnosis code, date of last menstrual period, mammography-certification number, family-planning indicator, patient primary identifier, subscriber current weight, subscriber previous weight, reason for last visit, occupation code, prognosis code, service-type code, surgical-procedure code, and hundreds of additional items of intensely personal information.

Unique identifiers for employers, providers, and patients are also required for the standard transactions. HHS has proposed as the "national standard employer identifier" the employer identification number (EIN)—that is, the employer's "taxpayer identifying number"—stating that "each health care provider must use the national employer identifier whenever required on all transactions the health care provider transmits electronically" and that health plans and health care clearinghouses must use the EIN whenever required as a data element on standard transactions (U.S. Dept. of HHS HCFA 1998b, 32798). Another proposed HHS rule would require health plans, health care clearinghouses, and health care providers to use as their unique identifiers the "national provider identifier" supported by the Health Care Financing Administration (HCFA), consisting of "an 8-position alphanumeric identifier, which

includes as the eighth position a check digit" (U.S. Dept. of HHS HCFA 1998c, 25356). This proposed rule would require each health care provider to "obtain, by application if necessary, a national provider identifier," ordering all covered entities to supply and use national provider identifiers for all standard transactions.

More contentious are the HIPAA-mandated unique health identifiers for every American. Many people recoiled in 1998 when HHS issued a "White Paper" describing the alternate forms that the unique identifier might take, including biometric identifiers such as retinal-pattern analysis, iris scans, and voice-pattern analysis, among other candidate identifiers (U.S. Dept. of HHS 1998, sec. III[C]; Twight 1999, 182–84). When Congress later postponed implementation of the identifiers on a year-by-year basis,[2] privacy advocates expressed hope that eventual congressional repeal of the mandate for unique health identifiers might yet protect our medical privacy.

It is a vain hope. Even if Congress, bowing to political pressure by privacy groups, "permanently" prohibited creation of new identifiers, our medical records would still carry a unique health identifier: namely, the Social Security number (SSN) that health care providers for years have demanded and used to identify our records. HHS itself listed the SSN as a candidate identifier, citing its status as "the current de facto identifier" as an advantage of its use. With or without *new* identifiers, medical privacy thus remains in jeopardy. Either way, the HIPAA-envisioned system of standardized, widely shared personal medical information will proceed unimpeded. Ironically, repeal of the new identifier requirement, though not negating the threat to medical privacy, might even encourage public acquiescence to the emerging federal health information system.

Whatever the chosen patient identifier, with our detailed medical histories transcribed into standard transactions and formatted with standard data elements and uniform codes as the new regulations require, a treasure trove of personal information about each of us will exist in an easily manipulable and transferable form. The proffered shield against devastating abuse of this information is the HHS final rule, "Standards for Privacy of Individually Identifiable Health Information," which took effect April 14, 2001 (U.S. Dept. of HHS OPE 2000). Do these privacy standards create an effective shield, or are they instead a sieve through which individually identifiable health information can readily pass?

HHS Medical Privacy Rules: Shield or Sieve?

For those who have learned about the HHS medical privacy rules through the popular media, the answer would seem clear. The *New York Times,* for example, reported the forthcoming final rules under the heading "U.S. Plans Tighter Rules on Medical

2. For the December 2000 postponement, see *Consolidated Appropriations Act, 2001*, Public Law 106-554, 106th Cong., 2d sess., December 21, 2000, 114 Stat. 2763 (H.R. 4577), Appendix A, §514 at 114 Stat. 2763A-71. Section 514 states in its entirety: "None of the funds made available in this Act may be used to promulgate or adopt any final standard under section 1173(b) of the Social Security Act (42 U.S.C.

Files' Privacy" (Pear 2000). Another article described the final HHS rules as "even more protective of consumers' privacy than the Clinton administration had at first proposed, prompting the industry to increase its objections" and creating what consumer advocates regarded as "a milestone in the history of American medicine, the first comprehensive federal standards for medical privacy" (Pear 2001, A17). Again and again the media echoed the HHS summary of the rule, which proclaimed that "the use of these standards will improve the efficiency and effectiveness of public and private health programs and health care services by providing enhanced protections for individually identifiable health information" (U.S. Dept. of HHS OPE 2000, 82462). Indeed, it is difficult to find in the popular press any report that questions the strength of these privacy protections or suggests their privacy-eroding impact.

One has to read the regulatory fine print, lots of it, to see the holes. As I show here, the planned result of the regulation is not medical privacy. Rather, the language of privacy provides window-dressing intended to legitimize the nationwide standardization of medical data that will facilitate access to personal medical information on a scale never before experienced in the United States. Playing the central roles are:

- overbroad exemptions that allow individually identifiable health information to be used without the patient's consent or authorization;
- redefinition of the term *consent* in the regulation in ways that eviscerate its meaning;
- authorization of largely unimpeded medical-data sharing among government agencies; and
- failure to restrict redisclosure of individually identifiable health information by recipients that are not "covered entities."

While continuing to proclaim the "importance of privacy" and to assert that "privacy is a fundamental right," HHS created a rule that dramatically reduces the medical privacy of all Americans (U.S. Dept. of HHS OPE 2000, 82464). Unfortunately, the banner of "privacy" has been waved to marshal public support for federal rules that actually portend privacy's demise.

First, some terminology. The basic structure of the HHS privacy rule distinguishes *consent* from *authorization* for the use or disclosure of individually identifiable health information (called "protected health information"), and it further distinguishes disclosures with either consent or authorization from those without such permission. *Consent,* by definition, pertains to the disclosure of protected health information to "carry out treatment, payment, or health care operations" (U.S. Dept. of

1320d-2[b]) providing for, or providing for the assignment of, a unique health identifier for any individual (except in an individual's capacity as an employer or a health care provider), until legislation is enacted specifically approving the standard." Congress first passed measures delaying promulgation of such identifiers in the fall of 1998.

HHS OPE 2000, 82805, §164.502). *Authorization* pertains to the disclosure of protected health information for purposes other than treatment, payment, or health care operations. Contrary to apparent restrictions in HIPAA, the HHS privacy rule defines *protected health information* expansively to include not only records transmitted by or maintained in electronic media but also information "transmitted or maintained in any other form or medium," thereby putting the paper records of our medical histories within the rule's domain.[3] Similarly, the term *health care operations* is broadly defined to include even such activities as organizational fund-raising and the marketing of medical products and services (U.S. Dept. of HHS OPE 2000, 82803-4, §164.501).

Covered entities—health care providers, health plans, and health care clearinghouses—are allowed to use or disclose protected health information to carry out treatment, payment, or health care operations either *(a)* with the valid consent of the subject individual or *(b)* without his consent if the use or disclosure falls within the listed "exceptions" to the consent requirement. Likewise, covered entities may use or disclose protected health information for purposes other than treatment, payment, or health care operations either with the valid authorization of the subject individual or without his authorization if the use or disclosure falls within the listed "exceptions" to the authorization requirement.

Therefore, two pivotal issues are the meaning of *consent* and *authorization* under the HHS regulation and the scope of the exceptions to the consent/authorization requirements.

Consent, Authorization, and Opportunities to Object

Consider first the situations in which the HHS privacy regulations require the patient's consent as a precondition for disclosure of his medical information. Apart from the exceptions to be discussed later, the general rule is that a health care provider "must obtain the individual's consent, in accordance with this section, prior to using or disclosing protected health information to carry out treatment, payment, or health care operations" (U.S. Dept. of HHS OPE 2000, 82810, §164.506[a]). So far so good.

Next, however, the regulations state that a covered health care provider "may *condition treatment* on the provision by the individual of a consent under this section," and that a health plan "may *condition enrollment* in the health plan on the provision by the individual of a consent under this section sought in conjunction with such enrollment" (U.S. Dept. of HHS OPE 2000, 82810, §164.506[b], my empha-

3. U.S. Dept. of HHS OPE 2000, 82805, §164.501. HHS explained, "In this final rule we expand the definition of protected health information to encompass all individually identifiable health information transmitted or maintained by a covered entity, regardless of form." HHS averred that it wanted to "emphasize the severability of this provision," structuring the definition so that if a court disagreed with its view that HHS has "ample legal authority to cover all individually identifiable health information transmitted or maintained by covered entities," the overall rule would remain in operation (U.S. Dept. of HHS OPE 2000, 82496).

sis). In other words, although all health care providers and health plans are required to obtain consent in these cases, they can refuse to provide services unless this "consent" is forthcoming. Under the HHS privacy regulations, the patient therefore has no meaningful choice about this so-called consent; the patient's only available alternative is to forgo medical treatment. Our health care providers will offer us the following deal: cooperate and sign the consent form or be deprived of medical care. *Coerced consent* might be a more apt term.[4]

Moreover, the rules provide no assured legal channel by which a patient may restrict disclosure of personal medical information. Driving that point home, the regulation requires that a valid consent form must state that the "individual has the right to request that the covered entity restrict how protected health information is used or disclosed to carry out treatment, payment, or health care operations," but it adds that "the covered entity is *not required to agree to requested restrictions*" (U.S. Dept. of HHS OPE 2000, 82810, §164.506[c], my emphasis; see also 82822, §164.522). HHS was equally clear in explaining the patient's lack of a legal right to sue over violations of medical privacy. In response to public comments arguing that "individuals should be able to sue for breach of privacy," HHS stated, "We agree, but do not have the legislative authority to grant a private right of action to sue under this statute" (U.S. Dept. of HHS OPE 2000, 82566).

The rules regarding authorization resemble those regarding consent. The general rule is that covered entities "may not use or disclose protected health information" without a valid authorization (U.S. Dept. of HHS OPE 2000, 82811, §164.508). Compared to the consent regulations, the authorization rules more extensively restrict covered entities' ability to withhold medical services if a patient refuses to authorize disclosure of protected health information. Of course, there are exceptions, which allow the withholding of research-related treatment as well as the denial of enrollment and benefit eligibility if access to relevant information is not authorized. As with the consent regulations, however, the most significant exceptions are set forth in a separate section (to be discussed later).

Finally, a section labeled "Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object" deals with disclosures for facility (for example, hospital) directories and disclosures to family members and others directly involved in an individual's care. For such disclosures, this section removes the covered entity's obligation to obtain a patient's consent or authorization if the patient, given an opportunity to agree or object to a disclosure, does not object (U.S. Dept. of HHS OPE 2000, 82812, §164.510). The regulation states: "A covered entity may use or disclose protected health information *without the written consent or*

4. HHS itself stated that "concern about the coerced nature of these consents remains" (U.S. Dept. of HHS OPE 2000, 82473). As economist Paul Heyne once explained, to *coerce* is *"to induce cooperation by threatening to reduce people's options,"* whereas to *persuade* is to *"induce cooperation by promising to expand people's options"* (1997, 363, emphasis in original).

authorization of the individual . . . provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the disclosure in accordance with the applicable requirements of this section" (ibid., my emphasis).

Opening the door to unverifiable assertions of patient agreement in these circumstances, the regulation further states that the covered entity "may *orally* inform the individual of and obtain the individual's *oral agreement or objection* to a use or disclosure permitted by this section" (U.S. Dept. of HHS OPE 2000, 82812, §164.510, my emphasis). Although commenters expressed concern that the provision might allow the disclosure of the location of incapacitated victims of domestic violence and thereby increase their vulnerability to additional harm, HHS left such decisions to the professional judgment of health care providers acting in their patients' best interest, expressing the department's concern that "imposing an affirmative duty on institutions not to disclose information any time injuries to the individual could have been the result of domestic violence would place too high a burden on health care facilities" (U.S. Dept. of HHS OPE 2000, 82663).

Worries about the HHS privacy rule, however, do not stop here. Explicit legal power for our doctors and other covered entities to disclose our personal medical records without our permission is created by a subsequent section of the regulation that lists exceptions to the consent, authorization, and "agree or object" provisions.

Casting Consent Aside

The exceptions are large in number and scope. Mincing no words, HHS entitled section 164.512 "Uses and Disclosures for Which Consent, an Authorization, or Opportunity to Agree or Object Is Not Required" (U.S. Dept. of HHS OPE 2000, 82813). For each category listed, a "covered entity may use or disclose protected health information *without the written consent or authorization of the individual . . . or [without] the opportunity for the individual to agree or object*" (ibid., my emphasis). These exceptions include:

- Uses and disclosures required by law
- Uses and disclosures for public health activities
- Disclosures about victims of abuse, neglect, or domestic violence
- Uses and disclosures for health oversight activities
- Disclosures for judicial and administrative proceedings
- Disclosures for law enforcement purposes
- Uses and disclosures about decedents

- Uses and disclosures for cadaveric organ, eye, or tissue donation purposes
- Uses and disclosures for research purposes
- Uses and disclosures to avert a serious threat to health or safety
- Uses and disclosures for specialized government functions
- Disclosures for workers' compensation

All without permission. In each of these situations, a government that claims to be advancing medical privacy allows physicians, health insurance issuers, HMOs, Medicare program officials, and other covered entities legally to disclose medical records to those seeking them with no permission whatsoever from the patient.

In addition, the regulation grants the HHS secretary unlimited access to covered entities' records without patient consent, mandating that covered entities maintain whatever records HHS requires and give HHS access to those records on demand. These records explicitly include individually identifiable health information: "A covered entity must permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, *including protected health information,* that are pertinent to ascertaining compliance" (U.S. Dept. of HHS OPE 2000, 82802, §160.310[c], my emphasis). One wonders what health information could escape being deemed "pertinent to ascertaining compliance." Moreover, reflecting a more general problem to be discussed later, HHS redisclosure of these records is permitted whenever it is either required by law or deemed necessary in the interest of assuring compliance.

Despite public animosity to government acquisition of personal medical records, government entities are the primary recipients of that information under the listed exceptions. Whether in the name of compliance, health oversight, public health, law enforcement, or other listed rationales, the HHS privacy rules make our medical records an open book to government officials. The exceptions listed in §164.512 provide a legal pretext for virtually unchecked disclosure of our personal medical histories to government entities and, as we will see, for virtually unchecked redisclosure of that medical information by government agencies and others. Let us examine the exceptions in more detail.

Required by Law. Several interrelated provisions allow disclosures "required by law." The umbrella provision states that, without patients' permission, a covered entity "may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law" (U.S. Dept. of HHS OPE 2000, 82813, §164.512 [a]). Thousands of pages of federal statutes, regulations, and judicial decisions are swept into this single sentence. Evoking its broad reach, HHS defines "required by law" to mean:

> a mandate contained in law that compels a covered entity to make a use or disclosure of protected health information and that is enforceable in a court of law. *Required by law* includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits. (U.S. Dept. of HHS OPE 2000, 82805, §164.501, emphasis in original)

As this passage makes clear, when you want to know what lawmakers really want, read the definitions they write. The full range of government-mandated medical information lies within this provision's reach.

This umbrella provision is closely linked with other exceptions that deal with disclosures for law-enforcement purposes, for judicial and administrative proceedings, and for protection of victims of abuse.

Victims of Abuse. Although the desire to protect victims of abuse is laudable, this regulation's provisions pertaining to victims of abuse, neglect, or domestic violence are laced with possibilities for inappropriate release of potentially inaccurate personal medical information to government authorities.[5] Disclosure of personal medical information without the patient's permission here has no fixed bounds, resting instead on the "reasonable belief" of the physician or other covered entity. The rule states that in certain circumstances "a covered entity may disclose protected health information about an individual whom the covered entity *reasonably believes* to be a victim of abuse, neglect, or domestic violence *to a government authority, including a social service or protective services agency,* authorized by law to receive reports of such abuse, neglect, or domestic violence" (U.S. Dept. of HHS OPE 2000, 82814, §164.512[c], my emphasis).

Despite our compassion for victims of abuse, with this broad language the specter of misinformation in the hands of social service agencies looms large. Disclosure may occur whenever it is either required by law, agreed to by the subject individual, or "expressly authorized by statute or regulation." Because what is "authorized" is broader than what is "required" by law, disclosure that is merely authorized is allowed only if *(a)* in the "professional judgment" of the covered entity disclosure is "necessary to prevent serious harm" to potential victims or *(b)* in circumstances of victim incapacity an authorized public official "represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure

5. This exception does not deal with child abuse, which is covered elsewhere.

would be materially and adversely affected by waiting until the individual is able to agree to the disclosure" (U.S. Dept. of HHS OPE 2000, 82814, §164.512[c]). Discretionary decision making—professional judgments and representations as easily shaped by misinformation or personal agendas as by altruism—thus may trigger release of damaging personal medical information, without the patient's permission, into public databases potentially shared with other interested parties.

Law Enforcement Purposes. Another exception allows covered entities to disclose individually identifiable medical records, without patient permission, for certain law enforcement purposes, authorizing disclosure to law enforcement officials when required by law or in response to various types of court orders and subpoenas. Its loosest provision allows disclosure of medical records in response to a mere "administrative request" that is "authorized by law" (authorized, not required), provided that three conditions are met: the information is "relevant and material to a legitimate law enforcement inquiry"; the request is "specific and limited in scope to the extent reasonably practicable"; and "de-identified information could not reasonably be used" (U.S. Dept. of HHS OPE 2000, 82815, §164.512 [f]). When administrative subpoenas are involved, HHS states that "this rule does not require judicial approval of administrative subpoenas," adding that administrative agencies can "avoid the need for judicial review by issuing subpoenas for protected health information only where the three-part test [described above] has been met" (U.S. Dept. of HHS OPE 2000, 82683). In the three-part test, as throughout the HHS regulation, slippery words such as *reasonably* erode seeming limitations on government authority.[6]

Judicial and Administrative Proceedings. A separate exception specifically allows disclosures of individually identifiable medical records without patient consent in conjunction with judicial and administrative proceedings, with or without the order of a court or administrative tribunal. Absent such an order, covered entities may disclose the information in response to lawful process, provided that those seeking the information give "satisfactory assurance" that "reasonable efforts have been made" either to notify the subject individual or to secure a protective order preventing disclosure beyond the scope and purpose of the litigation (U.S. Dept. of HHS OPE 2000, 82814–15, §164.512[e]).

Public-Health Activities. The broad language of this exception allows physicians and other covered entities to disclose individually identifiable medical records, without patients' permission, to countless public-health authorities for a wide range of purposes. Public-health authorities include not only all federal or state government agencies whose mandate includes "public health matters," but also government contractors and

6. Covered entities also can disclose personal medical records of "suspected" victims of crime to law enforcement officials without consent in emergency circumstances if the official represents that the information is "needed to determine whether a violation of law by a person other than the victim has occurred" and that "immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure" (U.S. Dept. of HHS OPE 2000, 82815–16, §164.512[f][3]).

others acting under "grant of authority" from such government entities (U.S. Dept. of HHS OPE 2000, 82805, §164.501). And the purposes for which such disclosure is allowed? According to HHS regulations, the legitimizing purpose is "preventing or controlling disease, injury, or disability," described as including such broad categories as "public health surveillance" and "public health investigations" (U.S. Dept. of HHS OPE 2000, 82813, §164.512[b]). Permitted disclosures also include those related to "child abuse or neglect," those related to certain Food and Drug Administration (FDA) product-tracking and recall programs, and those made to people "who may have been exposed to a communicable disease" (U.S. Dept. of HHS OPE 2000, 82813–14).

Health Oversight Activities. Equally expansive is the exception allowing disclosure of individually identifiable medical records, without patients' permission, for the purpose of health oversight. The provision's breadth is astonishing. It states that covered entities may disclose our medical records to any "health oversight agency" for oversight activities authorized by law:

> including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:
>
> (i) The health care system;
>
> (ii) Government benefit programs for which health information is relevant to beneficiary eligibility;
>
> (iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or
>
> (iv) Entities subject to civil rights laws for which health information is necessary for determining compliance. (U.S. Dept. of HHS OPE 2000, 82814, §164.512[d])

According to its own terms, this section is not supposed to be invoked against an individual who is the subject of an investigation unless the investigation is directly related to the person's "receipt of health care" or to claims for public benefits dependent on the individual's health. Even this protection crumbles, however, because of subsequent language stating that for joint health-oversight investigations involving a "claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity" that allows disclosure of medical information.

Serious Threat to Health or Safety. Covered entities also may disclose individually identifiable medical information without the patient's permission if the covered entity "in good faith" believes the disclosure either is necessary to reduce a "serious and imminent" threat to health and safety or, in certain cases, is "necessary for law enforcement authorities to identify or apprehend an individual" (U.S. Dept. of HHS OPE 2000, 82817, §164.512[j]). The requisite good faith is presumed in the regula-

tion provided that the covered entity has acted based on a "credible representation by a person with apparent knowledge or authority."

Research Purposes. HHS regulations pertaining to the use of medical records for research purposes provide other avenues through which privacy may be compromised. The basic idea is to allow doctors and other covered entities to disclose medical records, without the patients' permission, for research purposes, provided that the covered entities follow specified procedures for institutional review and approval of their actions. But the criteria for releasing and the procedures for protecting medical records in these circumstances are riddled with subjective language susceptible to serious breaches of medical privacy.

Covered entities may release individually identifiable medical records to publicly or privately funded researchers without patient authorization provided that the covered entities have obtained approval from either *(a)* an Institutional Review Board (IRB) established in conformity with existing federal regulations or *(b)* a "privacy board" as described in the HHS privacy rule. Least stringent is the latter option. Although prohibiting board members from reviewing any project regarding which they have a conflict of interest, the HHS regulations require only *one* member on the privacy board "who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any such entities" (U.S. Dept. of HHS OPE 2000, 82816, §164.512[i]).

The criteria for approval? Mere assertions by the IRB or privacy board will do, statements that disclosure of medical records without patient permission:

- "involves no more than minimal risk to the individuals";
- "will not adversely affect the privacy rights and welfare of the individuals";
- is necessitated by "research [that] could not practicably be conducted without the alteration or waiver" of patient permission requirements and "without access to and use of the protected health information";
- creates "privacy risks to individuals . . . [that] are reasonable in relation to the anticipated benefits *if any* to the individuals, and the importance of the knowledge that may reasonably be expected to result";
- is accompanied by an "adequate plan to protect the identifiers from improper use and disclosure" and "an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, *unless there is a health or research justification for retaining the identifiers,* or such retention is otherwise required by law." (U.S. Dept. of HHS OPE 2000, 82816, §164.512[i], my emphasis)

Likewise satisfied by properly formatted assertions and plans, a final criterion requires "adequate written assurances that the protected health information will not be reused

or disclosed to any other person or entity" except as required by law for "authorized oversight of the research project" or for "other research for which the use or disclosure . . . would be permitted" (U.S. Dept. of HHS OPE 2000, 82816–17).

Moreover, even before obtaining IRB or privacy board approval for access to individually identifiable medical records without patient permission, prospective researchers engaged in formulating a research project may be granted such access by a covered entity on the strength of mere assurances that the information is necessary and will not be used inappropriately. A covered entity is only required to obtain a researcher's "representations" that the disclosure sought is "necessary to prepare a research protocol or for similar purposes preparatory to research," that "no protected health information is to be removed from the covered entity," and that the disclosure "is necessary for the research purposes."[7] What prospective researcher would not proffer such representations?

A shortcut review process is available for privacy boards examining researchers' requests for medical information. The board may elect to use this "expedited review procedure" if it is claimed that the research "involves no more than minimal risk to the privacy of the individuals" whose medical records are being sought. In this procedure, the determination of whether to release your medical records without your permission can be made by a single individual: "If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair" (U.S. Dept. of HHS OPE 2000, 82817, §164.512[i]). One person, subjective criteria, and no representation of the individuals whose records are involved: under these regulations, it's the law.

In addition to the exceptions just listed, the rules also state that covered entities may use or disclose certain individually identifiable health information, without authorization by the patient, for fund-raising and marketing purposes. A covered entity may release "demographic information relating to an individual" and "dates of health care provided to an individual" for "the purpose of raising funds for its own benefit, without an authorization" by the individual patient, provided that the fund-raising solicitation describes how the recipient can opt out of receiving future fund-raising communications (U.S. Dept. of HHS OPE 2000, 82820, §164.514[f]). Likewise, covered entities may divulge individually identifiable health information without the individual's authorization for the purpose of marketing "health-related products and services." The rules require only that opt-out instructions be included with the marketing solicitation, along with identification of the covered entity, description of any remuneration it is receiving for making the communication, and explanation of "why the individual has been targeted and how the product or service relates to the health of the individual" (U.S. Dept. of HHS OPE 2000, 82819, §164.514[e]).

The fine print concerning other exceptions—for disclosures related to workers' compensation and for those involving decedents, including cadaveric organ, eye, or

7. Even fewer barriers to research-related disclosure shield medical information pertaining to deceased individuals (U.S. Dept. of HHS OPE 2000, 82816, §164.512[i]).

tissue donations—I do not examine here. However, the exception for "specialized government functions" must be reviewed, for it lies at the heart of the medical-data sharing authorized by the HHS rule.

Sharing Medical Information between Government Agencies: Uses and Disclosures for "Specialized Government Functions"

At first glance, the exception for "specialized government functions" may appear innocuous. It identifies exceptions to patient consent and authorization requirements for certain disclosures of medical information to government agencies in connection with military personnel management, national security and intelligence activities, protection of the president, State Department determinations of medical suitability, and the like. Tucked at the end of this exception, however, on the twenty-first page of the HHS regulation's fine print, is a provision that facilitates virtually unfettered sharing of our medical information between government agencies.

This provision allows certain government health plans, such as Medicare or the State Children's Health Insurance Programs (SCHIP), to disclose individually identifiable medical records to other government agencies without patient consent. Its first sentence states:

> A health plan that is a government program providing public benefits may disclose protected health information relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies *or the maintenance of such information in a single or combined data system accessible to all such government agencies* is required or expressly authorized by statute or regulation. (U.S. Dept. of HHS OPE 2000, 82818, §164.512[k][6], my emphasis)

In other words, patient information may be shared between government agencies and combined with data from other government agencies in a comprehensive data system whenever such disclosure is merely authorized (not necessarily mandated) by statute or regulation. HHS chose to put its imprimatur—in the name of privacy!—on the widespread sharing of personal medical data without patients' consent, endorsing this behavior rather than restricting it.

Nor is that all. The second and final sentence of the provision extends this approval to all "covered entities"—not only health plans but also health care providers and clearinghouses—that are government agencies:

> A covered entity that is a government agency administering a government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of

> protected health information is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs. (U.S. Dept. of HHS OPE 2000, 82818, §164.512[k][6], my emphasis)

Make no mistake: the result is a validation of the existing widespread sharing of people's medical information, without their consent, among a broad array of government programs, including Social Security, Medicare, Medicaid, and even the food stamp program. In its own explanation of the first sentence of this provision, HHS describes the approved data exchanges as follows:

> For example, section 1137 of the Social Security Act requires a variety of public programs, including the Social Security program, state medicaid programs, the food stamp program, certain unemployment compensation programs, and others, to participate in a joint income and eligibility verification system. Similarly, section 222 of the Social Security Act requires the Social Security Administration to provide information to certain state vocational rehabilitation programs for eligibility purposes. In some instances, it is a covered entity that first collects or creates the information that is then disclosed for these systems. *We do not prohibit those disclosures.* (U.S. Dept. of HHS OPE 2000, 82541, my emphasis)

Though HHS insists that the information can be shared only for eligibility determinations and not for other purposes, there is no mechanism in place to enforce such fine distinctions. Once the data are shared, a single computer keystroke can evade even the purest of regulatory intentions.

Regarding the second sentence of the regulatory provision just quoted, HHS is equally explicit about the scope of allowed data exchanges:

> For example, in some states, the Medicaid program and the State Children's Health Insurance Program are administered by different agencies, although they serve similar populations. . . . This provision would permit the covered entities administering these programs to share protected health information of program participants to coordinate enrollment and services and to generally improve the health care operations of the programs. (U.S. Dept. of HHS OPE 2000, 82541)

Although HHS again claims that this provision "does not authorize agencies to use or disclose" the shared health information for other purposes, such protestations are hollow in the absence of a viable enforcement mechanism (U.S. Dept. of HHS OPE 2000, 82541–42). Who exactly will stop them?

Rather than protecting the privacy of our medical records, this provision—explicitly allowing disclosure of our medical records, without our permission, between "government programs providing public benefits"—reinforces and validates

a growing array of disclosures undertaken by Congress and federal regulatory agencies. Even these disclosures, however, represent but the tip of the iceberg.

Uncontrolled Redisclosure of Medical Information

The threat to privacy that the HHS regulations pose is multiplied a thousandfold by the redisclosures of our medical records that they permit. As we have seen, the regulations enumerate the many categories of recipients to whom doctors and other covered entities may legally transfer our medical records, either with or without our consent or authorization. These recipients include many individuals and organizations that are not themselves covered entities. A giant hole in the regulations, which the HHS repeatedly acknowledges, is that they do not control most *re*disclosure of our medical records by authorized recipients who are not covered entities. As a result, the nationwide cornucopia of standardized personal medical information now being created will be disclosed to thousands of parties whose subsequent redisclosure of the information is wholly uncontrolled.

At the heart of the redisclosure problem is a provision allowing disclosure of patients' medical records, without their consent, to "business associates" of covered entities. A *business associate* is defined as any person who, on behalf of a covered entity, either *(a)* helps to perform a "function or activity involving the use or disclosure of individually identifiable health information"—functions such as claims processing, claims administration, data analysis, utilization review, quality assurance, billing, benefit management and the like—or *(b)* provides "legal, actuarial, accounting, consulting, data aggregation . . . , management, administrative, accreditation, or financial services" to the covered entity, "where the provision of the service involves the disclosure of individually identifiable health information from such covered entity" to the person (U.S. Dept. of HHS OPE 2000, 82798, §160.103). In short, when business relationships entail covered entities' disclosure of personal medical records to other firms, those other firms are regarded as business associates in the regulation. And many, perhaps most, business associates are not covered entities under the HHS rules: they are ordinary firms.

Because HHS has no direct jurisdiction, under HIPAA, over business associates that are not covered entities, it has attempted to control them indirectly through the covered entities. The mechanism is a required business associate contract, whereby a covered entity must obtain "satisfactory assurance that the business associate will appropriately safeguard the information" (U.S. Dept. of HHS OPE 2000, 82806, §164.502[e]).[8] When a business associate is not a covered entity, however, enforcement of the contract is at best weak and indirect. All HHS can do

8. There are exceptions. No assurances need be given if the recipient is a health care provider involved in the treatment of an individual. In addition, certain disclosures by a health plan "that is a government program providing public benefits" escape the assurance requirement, as do some disclosures by group health plans and HMOs to the plan's sponsor (U.S. Dept. of HHS OPE 2000, 82806, §164.502[e]).

is discipline the covered entity that created the business associate relationship, but it will do that only if

> the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful: (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary. (U.S. Dept. of HHS OPE 2000, 82808, §164.504[e])

In other words, if a business associate misbehaves in these circumstances and the covered entity takes the HHS-mandated steps, the end result is that patients' medical records will have been made public without their consent, and HHS cannot do anything about it. These are supposed to be "privacy" regulations?

Many other recipients of medical records under the HHS privacy regulations also are not covered entities. Law enforcement officials, courts, government administrative agencies, health-oversight organizations, even coroners: none fits the HHS definition of covered entities. Consequently, they, too, can redisclose medical records virtually at will, even though they initially obtained those records without patient permission under one of the exceptions discussed in the preceding section of this article.

During the approval process, HHS fully understood the problem, mentioning it many times in response to comments on the proposed rule, but plunged ahead anyway. It was a deliberate decision, with officials bluntly acknowledging that "HHS does not have the authority to regulate re-use or re-disclosure of information by agencies or institutions that are not covered entities under the rule":

> we [HHS officials] do not intend for the rule's permissive approach to health oversight or the absence of specific documentation to permit the government to gather large amounts of protected health information for purposes unrelated to health oversight as defined in this rule, and we do not intend for these oversight provisions to serve as a "back door" for law enforcement access to protected health information. While we do not have the statutory authority to regulate law enforcement and oversight agencies' re-use and re-disclosure of protected health information, we strongly support enactment of comprehensive privacy legislation that would govern public agencies' re-use and re-disclosure of this information. (U.S. Dept. of HHS OPE 2000, 82674, 82689)[9]

This approach resembles handing a neighbor's child a loaded gun and then stating that you have no authority to control the child. It is good that HHS favors a more

9. Similar HHS statements with regard to the redisclosure of protected information are scattered throughout the record. See U.S. Dept. of HHS OPE 2000, 82672, 82681, 82682, 82683, 82687, 82688, and 82694.

comprehensive privacy rule and that its officials do not intend for the government and others to accumulate vast databases of personal medical information about Americans, but even the best of intentions cannot stop the predictable results of this HHS action.

In the name of medical privacy, the final HHS rule published December 28, 2000, and put into effect on April 14, 2001, has given us coerced consent, wide-ranging exceptions that allow disclosure of medical records to diverse recipients without patients' permission, extensive sharing of people's medical records between government agencies, and virtually uncontrolled redisclosure of medical records by recipients—governmental and nongovernmental—that are not covered entities. Yet this very rule is said to protect us from the threat to our privacy posed by the nationwide standardization of our medical records mandated by Congress through HIPAA and now partially implemented by HHS regulation. How can we understand the vast discrepancy between the rhetoric and the reality of the HHS medical privacy rule?

Patterns

The uncomfortable truth is that in formulating the final medical privacy rule, government officials employed the same tactics that they used in engineering passage of Medicare in 1965 and HIPAA in 1996 (Twight 1997, 1998). Lawmakers again relied on government manipulation of political transaction costs—strategies whose chief effect has been to raise the costs to ordinary citizens of resisting measures that increase the size and scope of government (Twight 1994). Among the forms of this behavior used in passing Medicare and HIPAA and later in formulating the medical privacy rule are misrepresentation, the tying of unpopular measures to popular ones, and incrementalism.

In the most recent case, the misrepresentation has been breathtaking. HHS described the purpose of the medical privacy rule as follows:

> (1) To protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information;
>
> (2) to improve the quality of health care in the U.S. by restoring trust in the health care system . . . ; and
>
> (3) to improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection. (U.S. Dept. of HHS OPE 2000, 82463)

Of these stated purposes, the only one accomplished by this rule is to give patients specific (though qualified) rights of access to their own medical records and the opportunity to request correction of errors in those records (U.S. Dept. of HHS OPE 2000, 82823–26, §§164.524, 164.526). As for "controlling the inappropriate use of

that information," "creating a national framework for health privacy protection," and "restoring trust in the health care system," the only way these regulations might restore such trust is if government officials make sure that people do not understand the rule's actual content.

HHS officials have tried to do so. They have described the new rule as "likely the largest single federal initiative to protect privacy," emphasizing patient consent and control over disclosure of medical records (U.S. Dept. of HHS OPE 2000, 82468). Who would oppose such seemingly beneficent objectives? Of course, that is the point: disguising the rule's actual content by asserting its devotion to medical privacy significantly raised the transaction costs to ordinary Americans of understanding the regulation and of taking political action to oppose the antiprivacy measures embedded in it.

Misrepresentation saturates the very vocabulary of the rule. Consider HHS's use of the phrase *protected health information* in provisions that allow covered entities to disclose patients' medical records without their permission. That phrase recurs throughout the provision that lists the twelve major situations in which covered entities "may use or disclose protected health information without the written consent or authorization of the individual" (U.S. Dept. of HHS OPE 2000, 82813, §164.512). For example: "A covered entity *may disclose protected health information* for the public health activities and purposes described in this paragraph to . . . [a] public health authority . . . ; [a] covered entity *may disclose protected health information* to a health oversight agency for oversight activities authorized by law" (U.S. Dept. of HHS OPE 2000, 82813–14, my emphasis). By defining *protected health information* as "individually identifiable health information" and then consistently using the former phrase, HHS reinforced an impression that personal medical information truly is "protected" health information under the rule, even as that information was stripped of protection in the normal sense of the word through provisions authorizing its disclosure without patients' permission.

More broadly, HHS asserted to the public that "until now, virtually no federal rules existed to protect the privacy of health information" and that the final rule "establishes, for the first time, a set of basic national privacy standards and fair information practices that provides all Americans with a basic level of protection and *peace of mind* that is essential to their full participation in their care" (U.S. Dept. of HHS OPE 2000, 82464, my emphasis). A nice touch, that: peace of mind.

Beyond the misrepresentation, as with the earlier HIPAA and Medicare legislation, here, too, the federal government tied unpopular measures to popular ones, presenting the whole as a package deal. Linking popular measures, such as patients' rights to examine and correct their own medical records, with less popular ones, such as disclosure of patients' medical records without their permission, again raised the political transaction costs of opposing a measure that increased the federal government's power.

Incrementalism also served that end, mirroring earlier U.S. experiences with HIPAA and Medicare, and prevailed on several levels. For one, HHS presented the HIPAA regulations piecemeal: first the transactions rule, then proposals for the provider and employer health identifiers, then the privacy rule, and so on. Because less is at stake in fighting each piece of the new structure than would be at stake if the entire structure were considered as a whole, incentives to resist the HIPAA-mandated regulatory system have been reduced accordingly. Moreover, incremental formulation of the regulatory package has allowed Congress to postpone until last the controversial HIPAA-mandated unique health identifier for every American, deflecting an issue that might have destroyed support for the new federalized health information system.

Incrementalism is also apparent in the sequence of steps involved in developing each individual HIPAA-mandated regulation. Each separate regulation entailed solicitation of public comments, often at multiple stages during the individual rule's development. For the transactions rule, the privacy rule, the proposed provider identifier rule, a forthcoming security rule, and the rest, the public was given opportunities to comment. HHS, in turn, generated hundreds of pages of published responses to the comments. In the end, it usually adjusted its language here and there to accommodate the public's comments, but generally secured the overall result it wanted anyway.

For example, the originally proposed privacy rule did not require patient consent for covered entities' use and disclosure of medical information, actually forbidding covered entities from obtaining such consent (U.S. Dept. of HHS OPE 2000, 82648–49). Many who commented on the proposal expressed deep concern—even outrage—at the lack of a consent provision. The HHS response? The department trimmed its sails to the prevailing winds by inserting a "consent" provision for health care providers, but eviscerated the provision by allowing providers to withhold treatment unless consent is given, mandating the form but not the substance of meaningful consent. Similarly, when the public complained about a proposed provision that would have allowed medical data dissemination without patients' permission for government health data systems, HHS deleted the offending provision but achieved much the same result in more subtle ways. Department officials acknowledged that the actual outcome was little changed:

> we agree with the commenters who suggested that the proposed provision that would have permitted disclosures to government health data bases was overly broad, and we remove it from the final rule. We reviewed the important purposes for which some commenters said government agencies needed protected health information, and *we believe that most of those needs can be met through the other categories of permitted uses and disclosures without authorization allowed under the final rule,* including provisions permitting covered entities to disclose information (subject to certain limitations)

> to government agencies for public health, health oversight, law enforcement, and otherwise as required by law. (U.S. Dept. of HHS OPE 2000, 82669, my emphasis)

Is it any wonder that opposition is eroded by such tactics? For grinding down opposition, incrementalism is a proven strategy.

Given the incrementalism, misrepresentation, and similar tactics that have been midwife to the federal controls that now enmesh U.S. health care, what is the prognosis for medical privacy in general and for the HHS privacy rules in particular?

Prospects

The outlook for medical privacy is bleak. When the Bush administration allowed the medical privacy rule to take effect, privacy advocates expressed hope that the rule's fundamental problems might be remedied by future modifications of offending provisions, but such melioration now appears unlikely. Although some revisions are to be expected, it is highly doubtful that the basic structure of the regulation will change—at least not at the government's own initiative.

If this view seems too pessimistic, consider the issue from the perspective of a congressional representative or senator. Envision a roll-call vote on these "standards for privacy of individually identifiable health information." Even knowing all that we know about the HHS rule, would most legislators choose to go on record opposing the measure, in hopes that they could somehow explain to their constituents why they voted to dismantle the "medical privacy rule"? That choice is the very one legislators would have faced if Representative Ron Paul (R.-Tex.) had succeeded in June 2001, under Congressional Review Act procedures, in bringing to a vote his proposal to repeal the rule (H.J. Res. 38).

Clearly, with adoption of the HHS medical privacy rule, political transaction costs have been shifted again. Strong political forces would be needed to change the new status quo in a fundamental way, but such opposition is unlikely to materialize—in part because this regulatory package has been falsely represented to the public as enhancing privacy, in part because of the usual realities of concentrated interest groups arrayed against dispersed citizens who, even if they understood the antiprivacy nature of the regulation, would have scant incentives as individuals to undertake costly political action. Obviously, the interest groups that expect to benefit from the government-mandated cornucopia of individually identifiable medical information will not readily relinquish their prize.

Political transaction costs of resisting this rule and other government-expanding measures will also change on a deeper level as a result of the privacy-destroying features of the new regulation. With government officials and others gaining greater access to personal medical histories under the rule, it will become increasingly possible for recipients of that information illicitly to threaten political and ideological adversaries with public revelation of embarrassing or damaging material gleaned from

those records. The long history of both Democratic and Republican administrations' official misuse of FBI and IRS records attests to this danger. As Richard Sobel of Harvard Law School has stated, "centralized information is centralized power" (quoted in Stolberg 1998, A13). With implementation of the HHS rule, centralized medical information will create more such power, increasing the political transaction costs of dissent on a broad range of public-policy issues.

If my analysis is correct, the rule's key provisions undermining medical privacy are likely to remain intact as diverse interest groups vie for modifications of the regulations. The language of consent will continue to be coupled with the reality of coercion. Laudable purposes such as law enforcement, domestic abuse prevention, efficient government administration, and the like will continue to mask the rule's overbroad exceptions to requirements for patient consent, enabling government entities to remain as the principal beneficiaries of the disclosures. The sharing of personal medical data among government agencies, already a reality, will not be forsworn. With regard to noncovered entities' redisclosure of medical records, as HHS has stated, the authority for extending privacy regulations to these recipients would require extensive new legislation, which is unlikely to be passed any time soon—and, as a practical matter, also unlikely to be enforceable even if enacted into law.

The chief—perhaps the only—hope on the immediate horizon is a lawsuit filed on July 16, 2001, challenging the HHS medical privacy rule on constitutional grounds. In a lawsuit against HHS and HHS secretary Tommy Thompson, plaintiffs in the case (physicians and medical societies in Louisiana and South Carolina) raise constitutional challenges to the HHS privacy regulation and to the HIPAA provisions authorizing it (Civil Docket No. 3:01-CB-2965, U.S. Dist. Ct., District of South Carolina Columbia Div., cited in Brase 2001). The outcome of that suit should be watched closely.

In the meantime, with the reshaping of political transaction costs surrounding the new federal health information system, the impending destruction of medical privacy becomes an ever more likely institutional reality. On July 6, 2001, HHS released more than thirty-five single-spaced pages of official "guidance" regarding implementation of the medical privacy rule, still denying that the rule expands government and law enforcement access to our medical records, except with regard to enforcement-related HHS access (U.S. Dept. of HHS OCR 2001, HIPAA Privacy TA 160.300.001).

HHS protestations notwithstanding, as I have shown, the medical privacy rule *does* ensure that Americans will be subjected to ever-increasing government access to their medical records without their consent, as well as to similar access by private companies acting with the blessing of the federal government. The only question is how soon this new mother lode of personal medical data will be fully exploited for private political and economic gain. Never mind that 92 percent of respondents to the September 2000 Gallup poll opposed government agencies' access to their medical records without their consent. By virtue of the Clinton/Bush medical privacy regula-

tions, these respondents have lost the battle, although even now they and most other people do not know it. Owing to those regulations, another part of our independence and autonomy has slipped away.

References

Brase, Twila. 2001. Lawsuit against HHS and Medical Privacy Rule Is Step in Right Direction. Citizens' Council on Health Care Press Release, July 16, St. Paul, Minnesota.

Gallup Organization. 2000. *Public Attitudes toward Medical Privacy.* Princeton, New Jersey: Gallup Organization.

Heyne, Paul. 1997. *The Economic Way of Thinking.* 8th ed. Upper Saddle River, N.J.: Prentice Hall.

Paul, Ron. 2001. Medical Privacy Threatened by Federal Health Bureaucrats. *Texas Straight Talk,* June 18. Available at: http://www.house.gov/paul/tst/tst2001/tst061801.htm.

Pear, Robert. 2000. U.S. Plans Tighter Rules on Medical Files' Privacy. *New York Times,* August 20, A14.

———. 2001. Medical Industry Lobbies to Rein in New Privacy Rules. *New York Times,* February 12, A1, A17.

Stolberg, Sheryl Gay. 1998. Health Identifier for All Americans Runs into Hurdles. *New York Times,* July 20, A1, A13.

Twight, Charlotte. 1994. Political Transaction-Cost Manipulation: An Integrating Theory. *Journal of Theoretical Politics* 6, no. 2: 189–216.

———. 1997. Medicare's Origin: The Economics and Politics of Dependency. *Cato Journal* 16, no. 3: 303–38.

———. 1998. Medicare's Progeny: The 1996 Health Care Legislation. *The Independent Review* 2, no. 3: 373–99.

———. 1999. Watching You: Systematic Federal Surveillance of Ordinary Americans. *The Independent Review* 4, no. 2: 165–200.

U.S. Department of Health and Human Services (HHS). 1998. *Unique Health Identifier for Individuals: A White Paper.* Washington, D.C.: U.S. Government Printing Office, July 2.

———. Health Care Financing Administration (HCFA). 1998a. Health Insurance Reform: Standards for Electronic Transactions. Proposed Rule, May 7. *Federal Register* 63: 25272 ff. (Summary and Background), 25305 ff. (Proposed Rule).

———. 1998b. Health Insurance Reform: National Standard Employer Identifier. Proposed Rule, June 16. *Federal Register* 63: 32784 ff. (Summary and Background), 32796 ff. (Proposed Rule).

———. 1998c. National Standard Health Care Provider Identifier. Proposed Rule, May 7. *Federal Register* 63: 25320 ff. (Summary and Background), 25355 ff. (Proposed Rule).

———. 2000. Health Insurance Reform: Standards for Electronic Transactions. Final Rule, August 17. *Federal Register* 65: 50312 ff. (Summary and Background), 50365 ff. (Final Rule).

U.S. Department of Health and Human Services (HHS). Office of the Assistant Secretary for Planning and Evaluation (OPE). 2000. Standards for Privacy of Individually Identifiable

Health Information. Final Rule, December 28. *Federal Register* 65: 82462 ff. (Summary and Background), 82798 ff. (Final Rule).

U.S. Department of Health and Human Services (HHS). Office for Civil Rights (OCR). 2001. OCR HIPAA Privacy Technical Assistance (TA), July 6. Available at: http://www.hhs.gov/ocr/hipaa/.