2002

HIPAA: Commercial Interests Win Round Two

Mike Hatch

HIPAA: Commercial Interests Win Round Two

Mike Hatch†

I. THE BANK PRIVACY PROVISION OF 1999: COMMERCIAL INTERESTS WIN ROUND ONE

Caught between the citizens' desire for autonomy and lobbyists representing commerce, federal policymakers capitulated to commercial lobbyists for the second time in three years by adopting HIPAA regulations. A brief review of the first round might shed light on the dynamics that produced HIPAA.

The first capitulation occurred in the fall of 1999, when Congress culminated a fifteen-year debate concerning the deregulation of banks by passing the Gramm-Leach-Bliley Act (GLB).[1] The debate focused on whether banks and their holding companies should be permitted to own commercial companies, such as securities and insurance firms. The affiliation of these firms had been expressly prohibited by the Glass-Steagall Act of 1933[2] and the Bank Holding Act of 1956.[3]

As Congress was nearing a final vote on the GLB, the State of Minnesota filed suit against US Bank National Association ND (US Bank).[4] The State alleged that US Bank violated consumer protection laws by misrepresenting to its customers that their account information was confidential.[5] In fact, the bank made over twenty pieces of information about each depositor

† Attorney General of Minnesota. Special thanks to the following staff of the Minnesota Attorney General's Office for their assistance on this Article: Assistant Attorney General Mark Ireland, Assistant Attorney General Erik Lindseth, Assistant Attorney General Margaret Chutich, Assistant Attorney General Jane Prine, and Administrative Assistant Renee Hansmeier.

1. Pub. L. No. 106-102, 113 Stat. 1338 (1999).

2. The Glass-Steagall Act is the name commonly used to refer to sections 16, 20, 21 and 32 of the Banking Act of 1933, 12 U.S.C. § 24 (1994 & Supp. II 1997), 12 U.S.C. §§ 78, 377-378 (1994).

3. 12 U.S.C. §§ 1841-1850 (1994 & Supp. II 1997).

4. Hatch v. US Bank Nat'l Ass'n ND, No. 99-872 (D. Minn. filed June 8, 1999).

5. *Id.*

available to telemarketers, including credit card numbers, account numbers, high balance, low balance, and customer profile designation.[6] The State alleged that the telemarketers then used this information to defraud customers by making unauthorized charges against their accounts.[7] The State's lawsuit against US Bank drew national attention to the issue of privacy when it came to light that most large banks in the United States also routinely sold their customers' personal financial information.[8]

Within days of the lawsuit's filing, bank lobbyists converged on Congress, which quickly responded by amending GLB to include a "bank privacy" provision.[9] Did this provision recognize an individual's right to financial privacy? Hardly.

The bank privacy provision permits banks to disclose personal financial data without depositor authorization to companies they own,[10] and to unrelated third parties if the purpose is to sell "financial products."[11] The provision conveniently does not define "financial products," which potentially gives even broader license for the bank to disclose data.

The bank privacy provision imposes one minimal obligation on financial institutions. Before distributing depositor data to other companies for non-financial products, banks must notify the depositor.[12] Banks do this by sending fine-print notices in bank statements, which are rarely read.[13] Even if the depositor

---

6. *Id.*

7. Hatch v. MemberWorks, Inc., No. MC99-010056 (Minn. Dist. Ct. filed Apr. 17, 2000).

8. Henry Gilgoff, *Private Matters: More Banks Now Selling Personal Consumer Data*, NEWSDAY, July 25, 1999, 1999 WL 8182389 ("[T]he deals are widespread among the country's biggest banks, [Comptroller of the Currency] Hawke said in a recent interview."). A U.S. Bancorp spokesperson stated that the "cooperative marketing programs are common practices." *Id.*; *see also* Dee DePass, *U.S. Bank Kills Marketing Deals*, STAR TRIB., June 11, 1999, at D1 (identifying Citibank's moratorium on sharing information with telemarketers); Marcy Gordon, *Chase Privacy Pact May Prompt Trend*, AP ONLINE, Jan. 28, 2000, 2000 WL 9751992 (stating that as many as twenty-two million consumers nationwide have been affected by Chase Manhattan's past decision to disclose personal customer information).

9. Robert O'Harrow Jr., *Bank Bill Privacy Provision Approved*, WASH. POST, June 11, 1999, at E1.

10. *See* 15 U.S.C. § 6802(a) (2000).

11. *Id.* § 6802(b)(2).

12. *See id.* § 6802(a) (citing § 6803(a)).

13. W.A. Lee, *Opt-Out Notices Give No One a Thrill*, AM. BANKER, July 10, 2001, at 1 ("'Many consumers have received their privacy notices, but because they are stuffed in the envelope with other materials and because

actually reads it, the fine print does not meaningfully explain what the financial institution intends to do with the depositor's sensitive financial information.[14] United States Senator Richard Shelby summarized GLB's privacy provisions as simply a "sham."[15]

Far from providing consumers with necessary protection, GLB's bank privacy provision legitimizes bank disclosure of depositor information. It is a legislative oxymoron.

In their article, Professors Lawrence Gostin and James Hodge glowingly describe HIPAA as a national privacy safeguard that protects the privacy of identifiable health information.[16] A better description of HIPAA would be that it is a regulatory oxymoron. Rather than providing consumers with necessary protection, HIPAA actually sanctions disclosure of patients' sensitive health information. The only difference between HIPAA and GLB's bank privacy provision is that commentators do not pretend that public policy had anything to do with the bank privacy provision.[17]

II. HIPAA SANCTIONS DISCLOSURE UNDER THE GUISE OF PRIVACY

HIPAA rules[18] only apply to health data if the patient can be identified in the data, such as by name, social security number, or other means.[19] In other words, as long as the patient identifier is suppressed, HIPAA allows medical data to be made public.[20] It can be blown up and put on a website, or otherwise

---

they're often in very fine print, customers are largely ignoring them,' said Beth Givens, director of the Privacy Rights Clearinghouse.").

14. *Id.* (noting that the privacy notices are "indecipherable").

15. Jeri Clausing, *Revised Banking Legislation Raises Concerns About Privacy*, N.Y. TIMES, Oct. 25, 1999, at C1.

16. *See generally* Lawrence O. Gostin & James G. Hodge, Jr., *Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule*, 86 MINN. L. REV. 1439 (2002) (describing HIPAA in favorable terms).

17. The nullification of financial privacy was simply the result of raw power being exercised by commercial lobbyists. *See* sources cited *supra* note 8; *see also* Rachel Zimmerman & Glenn R. Simpson, *Lobbyists Swarm to Stop Tough Privacy Bills in States*, WALL ST. J., Apr. 21, 2000, at A16. Public policy had nothing to do with the law. *Id.*

18. *See* 45 C.F.R. §§ 160-164 (2001).

19. *See id.* § 164.500 (noting that the regulations apply to "protected health information," which is defined generally in § 164.501 as "individually identifiable health information").

20. *See id.* § 164.514(a).

published.

Even if the patient identifier is included with the health data, HIPAA also permits the wholesale distribution of the material under certain circumstances. For instance, health information can be disclosed without a patient's authorization to a third party to telemarket or direct mail "health related products or services" and other "products or services of nominal value."[21] Furthermore, third parties can use the information to market any other product on a face-to-face basis.[22] If the patient does not request that the marketing firm stop the commercial use of this personal information during the marketing encounter, the information may be used for additional marketing purposes.[23] Given the low response rate by bank depositors to the "privacy notice" required by GLB,[24] it is unlikely that many patients will have the presence of mind during a telemarketing call to request that the information be suppressed.

Another instance in which HIPAA permits disclosure of patient information is when disclosure is to a federal, state or local government agency, or a private contractor of such agency, if the agency is authorized by law to collect data concerning disease prevention, communicable disease, child abuse, or adverse reactions to FDA regulated products.[25] In Minnesota, the Department of Health is authorized to receive such data from health providers.[26]

HIPAA also permits disclosure without patient authorization to research projects if the disclosure is approved by an Institutional Review Board (IRB).[27] To approve disclosure, the IRB must find that the research project will maintain and destroy the data so that the patient harm stemming from potential disclosure is outweighed by the presumed benefit of the information's addition to the research project.[28] Because IRBs are established by research-oriented facilities, the likelihood of patient advocacy is minimal.[29]

---

21. *Id.* § 164.514(e)(2).
22. *Id.* § 164.514(e)(2)(A).
23. *See id.* § 164.514(e)(3)(i)(C).
24. *Supra* text accompanying notes 12-13.
25. *See* 45 C.F.R. § 164.512(b) (2001).
26. *See* MINN. STAT. § 62J.301 (2000).
27. 45 C.F.R. § 164.512(i)(1)(i)(A) (2001).
28. *See id.* § 164.512(i).
29. *See id.* § 690.107 (2001) (listing characteristics that IRBs, like the one referenced in § 164.512(i)(1)(i)(A), must possess).

Finally, HIPAA has established limits on the information that can be disclosed in some situations.[30] Health providers may disclose such information without patient authorization to law enforcement officials if the disclosure is necessary to alert such officials to the location, commission, nature or perpetrator of a crime.[31]

Because HIPAA permits disclosure without patient authorization in the above instances, the purpose of the patient authorization requirement becomes marginalized. In those few instances where patient authorization is needed, HIPAA permits the health care provider to refuse treatment to a patient who does not sign an authorization form[32]—the "sign or die" provision. Most patients have an insurance or HMO contract that requires the patient to use a "primary care provider" to receive health coverage. Because HIPAA permits disclosure without patient authorization in several instances, and because it permits the primary care provider to refuse treatment if authorization is not given, HIPAA effectively neutralizes the patient's ability to restrict access to medical information.

III. THE GOSTIN-HODGE APPROACH TO HEALTH PRIVACY

HIPAA undercuts the paramount value of individual autonomy, which forms the basis of the "notice and consent" procedures commonly used today in the medical field. Gostin and Hodge justify HIPAA by asserting that the law should balance the need for individual anonymity with the communal interest in efficiency and scientific advancement:

> [W]here the potential for public benefit is high and the risk of harm to individuals is low, . . . public entities should have discretion to use data for important public purposes. Individuals should not be permitted to veto the sharing of personal information irrespective of the potential benefit to the public.[33]

Gostin and Hodge argue that the patient's desire for confidentiality should be subordinate to the community's interest in projects that use medical surveillance to detect health care fraud, to evaluate the efficacy of particular treatments or to save money by comparing treatment utilization of specific

30. *See id.* § 164.512(f).
31. *Id.*
32. *Id.* § 164.506.
33. Gostin & Hodge, *supra* note 16, at 1441.

health providers.[34]

Gostin and Hodge reject the inherent importance of privacy in our culture. Embodied in the Bill of Rights is the premise that there is no community or government interest legitimate enough to justify an unconsented, warrantless intrusion into the privacy of one's home, car, body, or telephone. Laws like HIPAA give commercial marketers access to data that our Constitution deems too sensitive, absent probable cause that a crime has been committed, to be routinely observed by the government. If the government can simply buy information from a data miner, the protections of the Fourth Amendment become marginal. Indeed, the Fourth Amendment "reasonable expectation of privacy" standard is eroded if the citizen now must anticipate that medical and financial records are widely accessible to the public.

As described below,[35] Gostin and Hodge also overemphasize the need to have patient identifiers attached to medical information that is disclosed to the government, researchers, and insurers. None of the literature supporting HIPAA's adoption gives an adequate rationale as to why a patient's name or social security number needs to be attached to medical information being disseminated through the myriad of databases in government and commerce.

IV. THE CULTURAL IMPORTANCE OF MEDICAL PRIVACY

When speaking about medical privacy, I ask participants to raise their hand if they have been treated for depression, drug abuse, alcoholism, sexually transmitted diseases, sterility, erectile dysfunction, yeast infections, abortion, or for mental health problems. The participants are always healthy: Nobody ever raises a hand. All I hear is a gasp from a crowd indignant that I would be so impertinent as to ask them to publicly disclose such information.

This reaction reflects a deeply imbedded value in American culture. Privacy—and the right of the individual to embrace dignity—is considered an essential ingredient to individual autonomy and a free society. Stripped of privacy, the citizen is subjected to embarrassment by neighbors, discrimination by employers, and humiliation from friends and relatives. For in-

34. *See generally id.*

35. *See* discussion *infra* Part VI.

stance, health information can be used to deny a mortgage application, a job promotion, or an insurance policy.

The basic constitutional framework of our country is that the government—our communal organization—has no right to our private information, except as expressly permitted in the Constitution. This structure reflects the underpinnings of our culture. Thoreau,[36] Huxley,[37] Orwell,[38] and Rand[39] represent two centuries of a strong cultural rejection of the notion that the community has a right to information undermining the personal dignity of the private citizen. The American contemporary culture has closely embraced the issue of privacy in movies,[40] websites,[41] and newspapers.[42] Indeed, the United States Supreme Court has repeatedly held that the Constitution recognizes a citizen's right to privacy under the Fourth, Ninth, and Fourteenth Amendments.[43] This right to privacy has been extended to issues involving marriage,[44] procreation,[45] contraception,[46] family relationships,[47] and child rearing and education.[48] For example, in *Griswold v. Connecticut*[49] the United States Supreme Court ruled that a marital relationship lies within "a zone of privacy created by several fundamental constitutional guarantees."[50] The Court also held in *Roe v. Wade*[51]

36. *See* HENRY DAVID THOREAU, WALDEN AND OTHER WRITINGS OF HENRY DAVID THOREAU (Brooks Atkinson ed., 1937).

37. *See* ALDOUS HUXLEY, BRAVE NEW WORLD (HarperCollins Publishers 1998) (1932).

38. *See* GEORGE ORWELL, NINETEEN EIGHTY-FOUR (Alfred A. Knopf, Inc. 1992) (1949).

39. *See* AYN RAND, ANTHEM (1946).

40. *See, e.g.*, CONSPIRACY THEORY (Warner Bros. 1997); ENEMY OF THE STATE (Touchstone Pictures 1998); THE TRUMAN SHOW (Paramount Pictures 1998).

41. For example, in March 2002 the MSN search engine returned 242 websites for the term "privacy."

42. Based on research done by the Minnesota Attorney General's Office, in 2001 the following publications and wire service published the following number of stories referring to the topic of privacy: *The Los Angeles Times*, 100; *The Washington Post*, 62; *The New York Times*, 53; *The Wall Street Journal*, 49; and The Associated Press: 252.

43. *See infra* notes 44-48.

44. Loving v. Virginia, 388 U.S. 1 (1967).

45. Skinner v. Oklahoma, 316 U.S. 535 (1942).

46. Eisenstadt v. Baird, 405 U.S. 438 (1972).

47. Prince v. Massachusetts, 321 U.S. 158 (1944).

48. Pierce v. Soc'y of Sisters, 268 U.S. 510 (1925).

49. 381 U.S. 479 (1965).

50. *Id.* at 485.

that the right to privacy, either grounded in the Constitution's concept of personal liberty or in the Ninth Amendment, includes a woman's decision to terminate her pregnancy.[52] Indeed, a woman who decides to have an abortion also has a right to privacy to keep that decision from others, including her partner.[53]

Most states, including Minnesota, have recognized a common law right to privacy, and its principles are described in the Restatement of Torts.[54] As Minnesota Chief Justice Kathleen Blatz stated,

> The right to privacy is an integral part of our humanity; one has a public persona, exposed and active, and a private persona, guarded and preserved. The heart of our liberty is choosing which parts of our lives should become public and which parts we shall hold close.[55]

Many states have also adopted a statutory right to privacy. For instance, in Minnesota there is statutory recognition of confidentiality concerning tax returns,[56] cancer victims,[57] alcohol or drug abuse program participants,[58] welfare participants,[59] students,[60] library patrons,[61] sexual assault victims,[62] agricultural assistance recipients,[63] pharmacy customers,[64] insurance information,[65] and patient charts.[66] The courts in most states also recognize the right to privacy as it relates to communications with clergy,[67] spousal partners,[68] and therapists.[69]

---

51. 410 U.S. 113 (1973).
52. *Id.* at 153.
53. Planned Parenthood v. Casey, 505 U.S. 833, 895 (1992).
54. RESTATEMENT (SECOND) OF TORTS § 652A-652E (1977).
55. Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 235 (Minn. 1998) (Blatz, C.J.).
56. MINN. STAT. § 290.611 (2000).
57. *Id.* § 144.69.
58. *Id.* § 254A.09.
59. *Id.* § 13.46.
60. *Id.* § 13.32.
61. *Id.* § 13.40.
62. *Id.* § 13.822.
63. *Id.* § 13.643(2).
64. *Id.* § 151.213.
65. *Id.* § 72A.502.
66. *Id.* § 144.335.
67. *E.g.*, State v. Orfi, 511 N.W.2d 464, 469-70 (Minn. Ct. App. 1994).
68. *E.g.*, Lundman v. McKown, 530 N.W.2d 807, 829 (Minn. Ct. App. 1995) (discussing the Minnesota marital privilege law).
69. *E.g.*, State v. Gullekson, 383 N.W.2d 338, 340 (Minn. Ct. App. 1986) (discussing the Minnesota psychologist privilege law).

Medical information is particularly intimate and personal. Full disclosure between a patient and physician is important to assure that the physician receives an accurate description of a patient's history and symptoms. If a patient knows that a physician may disclose a disease or injury, or its cause, that is humiliating, embarrassing, or possibly illegal, the patient may withhold information necessary for the physician to provide effective treatment.

Indeed, over 2500 years ago the Hippocratic Oath recognized the right to patient privacy as an absolute, and not a relative, value: "All that may come to my knowledge in the exercise of my profession or outside of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal."[70]

American culture strongly supports the privacy of medical information. A Harris Equifax survey regarding health information privacy found that ninety-six percent of Americans thought that federal legislation should designate medical information as "sensitive" and impose penalties for its disclosure.[71] Eighty-five percent of the respondents thought that protecting the confidentiality of medical records was "absolutely essential" or "very important" in health care reform.[72]

The Wisconsin Medical Association undertook a similar survey of Wisconsin citizens concerning the release of patient-identifying medical information to the Wisconsin Department of Health.[73] Eighty-two percent of survey respondents indicated that they did not want such information disclosed either to the government or to their employer.[74]

In 1999, a Wall Street Journal/NBC survey asked people what they feared most in the coming century. The response most often given—more than war, poverty, or the environ-

70. STEDMAN'S MEDICAL DICTIONARY 799 (Marjory Spraycar ed., 26th ed. 1995) (translating the entire Hippocratic Oath); *see also* MERRIAM-WEBSTER'S MEDICAL DESK DICTIONARY 297 (1993) (defining the Hippocratic Oath as "an oath that embodies a code of medical ethics and is usu[ally] taken by those about to begin medical practice").

71. ELECTRONIC PRIVACY INFORMATION CENTER, MEDICAL PRIVACY PUBLIC OPINION POLLS (citing HARRIS EQUIFAX, HEALTH INFORMATION PRIVACY SURVEY (1993)), http://www.epic.org/privacy/medical/polls.html.

72. *Id.*

73. *Medical Society Waging Effort to Block Implementation of Data Collection Law*, 8 Health L. Rep. (BNA) 821 (1999).

74. *Id.*

ment—was "the loss of privacy."[75]

Tellingly, nearly one in five people polled by the California Health Care Foundation stated that they withhold information from doctors or pay cash for medical services in an effort to limit the hospital or doctor's ability to disclose the information.[76]

V. MEDICAL DISCLOSURE CAUSES REAL HARM

There has never been a more important time to safeguard our medical privacy. The rapid growth of marketing databases, the regular news of accidental or purposeful disclosure of sensitive health information, and the potential misuse of such information to deny credit, employment, or insurance coverage has never been greater.

Currently, over 1000 private companies compile comprehensive databases about individual consumers, a tenfold increase in just five years.[77] On average, companies trade and transfer personal information about U.S. citizens every five seconds.[78] These companies do not engage in the marketing of products or the research of general demographic groups. Rather, they simply engage in data mining, gathering as much information as possible about each person. For example, the Medical Marketing Service (MMS) offers lists of people with particular medical conditions.[79] In 2000, MMS offered for sale nearly fifty lists of individuals suffering from different medical ailments.[80] For instance, MMS advertised for sale the names and addresses of 700,000 people who are clinically depressed, 900,000 women who have yeast infections and 1.1 million indi-

75. THE SENATE MAJORITY TASK FORCE ON THE INVASION OF PRIVACY 12 (2000), http://www.senate.state.ny.us/docs/nyspriv00.pdf; *see also* Albert R. Hunt, *Bright Past Kindles Nation's Hope*, WALL ST. J., Sept. 16, 1999, at A9 (describing the poll results).

76. Alissa J. Rubin, *Lobbyists Go Full Tilt in Bid to Ease Patient Privacy Rules*, L.A. TIMES, Mar. 24, 2001, at A1.

77. Robert O'Harrow Jr., *Data Firms Getting Too Personal?*, WASH. POST, Mar. 8, 1998, at A1.

78. Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 2 (2000).

79. *See* JOEL R. REIDENBERG, EXAMPLES OF THE SALE OF PERSONAL INFORMATION (1999) (containing MMS lists given as examples to the National Association of Attorneys General's Privacy Working Group).

80. *See id.*

viduals who have diabetes.[81] MMS also sells lists of people with Alzheimer's disease, heartburn, Parkinson's disease, and heart disease.[82]

Another data-mining company is Metromail Corporation, which collects more than 900 different pieces of information on individual consumers, dating back more than ten years.[83] The company was sued because it revealed personal information to Texas prison inmates who performed data entry for the company.[84] The database contained information including income, marital status, hobbies, medical ailments, and other items such as whether consumers used dentures, sleeping aids, or hemorrhoid remedies.[85]

Unauthorized disclosures or security breaches related to electronic health records have become more frequent. In Minnesota, a university researcher accidentally posted the names and psychological evaluations of children on the University of Montana's homepage.[86] An employee of the Florida Department of Health and Rehabilitation Services used a list of 4000 AIDS patients to screen potential sexual partners for himself and his friends.[87] A drug manufacturer revealed the e-mail addresses of individuals with depression, bulimia, and obsessive-compulsive disorder.[88] A congressional candidate's health records relating to her attempted suicide were faxed to a newspaper.[89] The parents of a dead child whose kidney was donated to another child were contacted by the parents of the recipient, asking whether the deceased child's family had any history of cancer.[90] The parents of the child who received the organs were able to request the information because a university errone-

81. *Id.*

82. *Id.*

83. Nina Bernstein, *Personal Files Via Computer Offer Money and Pose Threat*, N.Y. TIMES, June 12, 1997, at A1.

84. *Id.*

85. *Id.*

86. Maura Lerner & Josephine Marcotty, *Web Posting Has Health and University Officials Scrambling*, STAR TRIB., Nov. 8, 2001, at B1.

87. Sarah Tippit, *AIDS List Leak Causes Concern Over Security of Health Records*, CHI. SUN-TIMES, Oct. 14, 1996, at 22.

88. Robert O'Harrow Jr., *Prozac Maker Reveals Patient E-Mail Addresses*, WASH. POST, July 4, 2001, at E1.

89. AMITAI ETZIONI, THE LIMITS OF PRIVACY 141 (1999); CHARLES J. SYKES, THE END OF PRIVACY 106 (1999).

90. Telephone Interview with Kidney Donor's Parents (2001) (on file with author).

ously included anonymous donor names in a mass mailing.[91]

VI. THE ILLUSORY COMMUNAL INTEREST IN PATIENT IDENTIFIERS

HIPAA not only marginalizes the value of privacy, it overstates the necessity of attaching patient identifiers to medical information. Our culture has no objection to the transfer of medical charts with a redacted patient's name, social security number, or other identifier to track the response and progression of treatment for sexually transmitted disease, depression, chemical dependency, hemorrhoids, yeast infections, erectile dysfunction, or any other disease that might be the subject of ridicule or discrimination. One presumes that high tech data analyses can effectively process and measure the treatments and side effects without use of patient identifiers. For instance, the use of an identifier for each health provider, and a numeric subset code to be used for each patient of a provider, would seemingly be helpful to categorize each patient being treated.

The premise of HIPAA, however, is that such medical information is not enough. HIPAA presumes that patient identifiers must also be attached to medical records to conduct valid research. Researchers I have interviewed indicate that the primary research purpose of attaching the patient identifiers is to follow a patient if he transfers from one provider to the next. Yet researchers have failed to provide examples of situations where such patient identifier information was found to meaningfully expedite conclusions concerning the efficacy of a particular treatment. There are simply too many other personal variables missing on general medical charts that impede the value of such close tracking of a patient. In other words, while a macro analysis of the efficacy of treatments of the United States population might reveal certain trends, it cannot answer with certainty whether other factors not recorded on a medical chart affect the treatment outcome. Accordingly, the use of a patient identifier to track a patient from one physician to the next is hardly necessary if only a general trend can be ascertained.

HIPAA also permits a government agency, and companies that contract with a government agency, to receive patient identifying health data without the patient's consent. HIPAA

91. Josephine Marcotty, *Names of Donors Are Accidentally Included in Letter to Kidney Patients*, STAR TRIB., Jan. 15, 2002, at A1.

allows government agencies to collect and share such information in a variety of ill-defined categories, such as any use "required by law,"[92] "public health activities,"[93] or "health oversight."[94] Yet, at no time do the proponents of HIPAA articulate the communal interest in using the patient's name to assemble and track such information. If the government accumulation of private health data pursuant to these categories is for medical research purposes, then the exception for government-sponsored medical research is nullified. If it is to assist the investigation and prosecution of criminal activity, then the exception for law enforcement purposes is unnecessary. If it is to monitor and evaluate the efficacy of treatment by health providers, the need for an identifier of the health provider, not the patient, should be sufficient. Rather than attempting to explain the value of, or need for, this communal interest, Gostin and Hodge cavalierly presume that the government has a "right" to access such information. This presumption contradicts the cultural value of privacy as expressed in the Constitution and in 200 years of common law.

Indeed, any attempt to justify HIPAA's disclosure rules as reflecting a balance of communal interest versus individual rights is undermined and laid bare by the rules that permit telemarketers to obtain private health data for marketing and fundraising purposes. Proponents of such rules should blush when they attempt to justify such activity on the basis of a "communal interest."

HIPAA proponents attempt to dress up their capitulation to commercial interests by concocting a communal interest, or a "governmental right to know," concerning health data. In fact, rules that permit disclosure of health data for purposes of telemarketing, fundraising, government snooping, and medical research can only be explained by looking to the many lobbyists and commercial interests that have a financial stake in obtaining such information. HIPAA should be recognized for what it is: a national policy promulgated by unelected government officials who succumbed to the interests of commercial enterprise and marginalized the citizen's right to privacy. The proponents of HIPAA represent a closely connected liaison of government agencies, pharmaceutical companies, law enforcement agencies,

92. 45 C.F.R. § 164.512(a) (2001).
93. *Id.* § 164.512(b).
94. *Id.* § 164.512(d)(1).

medical device manufacturers, and marketing companies. Their success in getting HIPAA adopted shows that their clout rivals that of the military industrial complex at the height of the Cold War.

CONCLUSION

Personal autonomy and liberty are the essence of privacy. Whether recognized in the Constitution, common law, or statute, the right to privacy empowers individuals to define, and redefine, who they are. This liberty interest recognizes that misuse of private information invades a person's privacy and may cause harm "far greater than could be inflicted by mere bodily injury."[95]

Two of the most important tools to preserve personal privacy are the right to receive notice concerning the disclosure of personal information and the right to withhold consent before such disclosure. HIPAA eviscerates the requirement that researchers or government agencies justify the disclosure of personal health information. It abandons any attempt to look for less intrusive methods to conduct such activities. By weakening notice and consent, the Gostin-Hodge approach marginalizes the value of personal autonomy and liberty.

The Gostin-Hodge approach also fails to address issues created by cross-industry ownership, such as a bank's ownership of an insurance company or an employer's sponsorship of a self-insured health plan. While such entities may have been separate twenty or thirty years ago, fewer boundaries now exist among banks, brokerages, pharmaceutical companies, hospitals, and insurers. This lack of industry segmentation increases the opportunity for personal health information to be misused, and further justifies the need to obtain express consent before health or medical information is disclosed.

Privacy is not only "the right to be let alone,"[96] but the right to define who we are as people by controlling the release of our private information. Today, this right to privacy or self-definition is increasingly threatened by advances in technology and the growing financial value of personal information. If we wish to truly protect our liberty interests consistent with deep-rooted public expectations for privacy, policymakers must

95. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890).

96. *Id.* at 195.

tighten the current HIPAA regulations and limit their exceptions. Only when the balance tips in favor of greater individual control do we fairly protect our liberty to choose "whether that which is [ours] shall be given to the public."[97]

97. *Id.* at 199.