2002

Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule

Lawrence O. Gostin
Georgetown University Law Center, gostin@law.georgetown.edu

James G. Hodge Jr.
Arizona State University

86 Minn. L. Rev. 1439-1479 (2002)

January 2010

Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule

86 Minn. L. Rev. 1439-1479 (2002)

Lawrence O. Gostin
Professor of Law
Georgetown University Law Center
gostin@law.georgetown.edu

James G. Hodge, Jr.
Professor of Health Law and Economics
Sandra Day O'Connor College of Law
Arizona State University
james.hodge.1@asu.edu

Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule

Lawrence O. Gostin†

James G. Hodge, Jr.††

INTRODUCTION

On April 12, 2001, President George W. Bush approved the Standards for Privacy of Individually Identifiable Health Information ("health data privacy regulations")[1] pursuant to a congressional mandate in the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[2] These regulations, promulgated by the Department of Health and Human Services (DHHS), represent the first systematic national privacy protections of health information. They protect the privacy of individually identifiable health records in any form (e.g., electronic, paper, and oral) through access, use, and disclosure limitations, fair information practices, and privacy and security policies.

† Professor of Law, Georgetown University Law Center; Professor, Johns Hopkins Bloomberg School of Public Health; Director, Center for Law and the Public's Health at Georgetown and Johns Hopkins Universities; Visiting Fellow, Centre for Socio-Legal Studies, Oxford University.

†† Adjunct Professor of Law, Georgetown University Law Center; Assistant Scientist, Johns Hopkins Bloomberg School of Public Health; Project Director, Center for Law and the Public's Health at Georgetown and Johns Hopkins Universities.

The Authors would like to acknowledge the research assistance of Mira S. Burghardt, J.D.; Gabriel B. Eber, M.P.H., J.D. Candidate, Georgetown University Law Center, 2004; and Marguerite Middaugh, B.A.

1. *See* Press Release, President George W. Bush (Apr. 12, 2001), *available at* http://www.whitehouse.gov/news/releases/2001/04/20010412-1.html; Press Release, Secretary Tommy G. Thompson, Statement by HHS Secretary Tommy G. Thompson Regarding the Patient Privacy Rule (Apr. 12, 2001), *available at* http://www.hhs.gov/news/press/2001pres /20010412.html.

2. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1997).

These provisions apply to all "covered entities" (i.e., health providers, health insurance plans, and health care clearinghouses) and their "business associates" (e.g., claims processors, billing managers, data analyzers, and others).[3]

National privacy safeguards are needed because of the proliferation of and access to health records resulting from the ongoing shift from paper to electronic records within the national health information infrastructure. The increasing potential to use or reveal sensitive health data raises concerns about privacy violations. Health information can include intimate details about the patient's mental and physical health as well as social behaviors, personal relationships, and financial status.[4] Polling data have consistently shown that Americans are concerned about the privacy of their medical data.[5] Over 80% of respondents in one survey suggested they had "lost all control over their personal information."[6] In another national survey, 78% of respondents felt it is very important that medical records be kept confidential.[7] Yet, there are multiple justifications for sharing health data to accomplish various communal interests. Sharing data may be necessary to achieve important health purposes (e.g., health research and public health) or for non-health-related purposes (e.g., the administration of justice and law enforcement).

We (and others) have previously suggested that health information privacy laws should carefully balance the need for individual privacy with the benefits of using health data for the common good.[8] For many, protecting the rights of individuals to control how their identifiable health data are accessed, used, or disclosed is the ultimate goal of national health information privacy standards. Individual interests in privacy, however,

---

3. *See infra* Part II.A for specific definitions of "covered entities" and "business associates."

4. *See* Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 489-90 (1995).

5. *See* Charles A. Welch, *Sacred Secrets—The Privacy of Medical Records*, 345 NEW ENG. J. MED. 371 (2001).

6. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,461 (Dec. 28, 2000) (citing Harris Equifax, *Health Information Privacy* (1999)), *available at* http://www.aspe.hhs.gov/admnsimp/final/PvcPre01.htm.

7. THE GALLUP ORG., INST. FOR HEALTH FREEDOM, PUBLIC ATTITUDES TOWARD MEDICAL PRIVACY 2 (2000).

8. *See, e.g.*, James G. Hodge, Jr., Lawrence O. Gostin & Peter D. Jacobson, *Legal Issues Concerning Electronic Health Information: Privacy, Quality, and Liability*, 282 JAMA 1466, 1470 (1999).

should not be regarded as absolute. Some disclosures of health data without specific informed consent are ethically appropriate and legally authorized, such as requirements to report infectious diseases to state health departments[9] and the duty to warn persons at significant risk of harm.[10]

The national privacy standards set a "floor" for protections that, DHHS suggests, "balance[s] the needs of the individual with the needs of the society."[11] Reaching this balance, however, is precarious. In some cases, the common good to be achieved is not worth the infringement of privacy. In other circumstances, the need for data may be sufficiently strong to outweigh the individual's claim to autonomy and privacy. Privacy laws at the federal, state, and local levels are fragmented and inconsistent, and do not reflect any coherent formula for balancing. In particular, the national privacy rule does not always achieve a fair and reasonable allocation of benefits and burdens for patients and the community.

We suggest rules for balancing private and public interests that go beyond the traditional conception of individual autonomy as a dominating factor. Rather than seeing autonomy as a "trump card" that always prevails, our framework values both privacy and common goods, without *a priori* favoring either. We instead seek to maximize privacy interests where they matter most to the individual and maximize communal interests where they are likely to achieve the greatest public good. Thus, where the potential for public benefit is high and the risk of harm to individuals is low, we suggest that 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. Privacy rules should not be so arduous and inflexi-

9. *See, e.g.*, Lawrence O. Gostin & James G. Hodge, Jr., *The "Names Debate": The Case for National HIV Reporting in the United States*, 61 ALB. L. REV. 679 (1998).

10. *See, e.g.*, Lawrence O. Gostin & James G. Hodge, Jr., *Piercing the Veil of Secrecy in HIV/AIDS and Other Sexually Transmitted Diseases: Theories of Privacy and Disclosure in Partner Notification*, 5 DUKE J. GENDER L. & POL'Y 9 (1998).

11. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,464 (Dec. 28, 2000). Electronic copies of the health data privacy rule, including background materials and comments published in the Federal Register, are available at http://www.aspe.hhs.gov/admnsimp or http://www.hhs.gov/ocr/hipaa. *See also* Andrew B. Wachler & Phyllis A. Avery, *Complex Privacy Regulations Have Far Reaching Impact*, 13 HEALTH LAW. 1, 3 (2001).

ble that they significantly impede, for example, health services research or surveillance necessary to promote the public's health. Provided that the data are used only for the public good (e.g., research or public health), and the potential for harmful disclosures are negligible, there are good reasons for permitting data sharing.

If the data, however, are disclosed in ways that are unlikely to achieve a strong public benefit, and the personal risks are high, individual interests in autonomy should prevail. For example, if health care professionals disclose personal health data to family, friends, neighbors, employers, or insurers, the public benefits to be achieved may not be worth the cost in personal privacy. Such disclosures can cause stigma and embarrassment. Disclosure to employers or insurers (e.g., health, life, or disability) can result in discrimination. These kinds of unauthorized disclosures can lead to a loss of patient trust in health care professionals. Individuals may be reluctant to seek medical treatment for some conditions (e.g., HIV/AIDS, other sexually transmitted conditions, or genetic diseases) or to disclose important information to health professionals.[12] Consequently, for these kinds of disclosures where the public benefits are negligible and individual privacy risks are high, the law should strictly prohibit the release of information without the patient's consent.

The framework for balancing we offer attempts to maximize individual and communal interests in the handling of identifiable health data. Acquisition, use, or disclosure of health information that can lead to harm would be subject to strict privacy protections. Correspondingly, acquisition, use, or disclosure of health information for important public purposes would be permitted provided that (1) uses are restricted to the purposes for which the data are collected, and (2) subsequent disclosures for other purposes are prohibited without individual authorization. This framework defends autonomy when individual interests are high and public interests are low. We recognize that adherence to this balancing test will entail a certain diminution of autonomy. However, it will be worth the cost in terms of the benefits that everyone will achieve in living in a society that values the communal goods offered by research, public health, and other public enterprises.

In this Article, we discuss how these principles for balanc-

12. *See* Gostin, *supra* note 4, at 490-91.

ing apply in a number of important contexts where individually identifiable health data are shared. In Part I, we analyze the modern view favoring autonomy and privacy. In the last several decades, individual autonomy has been used as a justification for preventing sharing of information irrespective of the good to be achieved. Although respect for privacy can sometimes be important for achieving public purposes (e.g., fostering the physician/patient relationship), it can also impair the achievement of goals that are necessary for any healthy and prosperous society. A framework for balancing that strictly favors privacy can lead to reduced efficiencies in clinical care, research, and public health. We reason that society would be better served, and individuals would be only marginally less protected, if privacy rules permitted exchange of data for important public benefits.

In Part II, we explain the national health information privacy regulations: (1) what do they cover?; (2) to whom do they apply?; and (3) how do they safeguard personal privacy? Parts III and IV focus on whether the standards adhere, or fail to adhere, to the privacy principles discussed in Part I. In Part III, we examine two autonomy rules established in the national privacy regulations: "informed consent" (for uses or disclosures of identifiable health data for health-care related purposes) and "written authorization" (for uses or disclosures of health data for non-health care related purposes). We observe that the informed consent rule is neither "informed" nor "consensual." The rule is likely to thwart the effective management of health organizations without benefiting the individual. Requiring written authorization, on the other hand, protects individual privacy to prevent disclosures to entities that do not perform health-related functions, such as employers and life insurers.

In Part IV, we examine various contexts in which data can be shared for public purposes under the national privacy rule: public health, research, law enforcement, familial notification, and commercial marketing. We apply our framework for balancing in each context and observe the relative strengths and weaknesses of the privacy regulations in achieving a fair balance of private and public interests.

I. DEVELOPING A FRAMEWORK FOR MAXIMIZING INDIVIDUAL PRIVACY AND COMMUNAL INTERESTS

A key priority of Congress in enacting HIPAA was to protect the privacy of identifiable health information. Congress

was concerned about the proliferation of health information and consumer loss of confidence in the health care system. Fundamental shifts in the organization, delivery, and financing of health care services were taking place. The integration of health service functions required the collection, storage, use, and disclosure of vast amounts of health data. Information was being shared among those who pay for (e.g., employers and insurers), provide (e.g., hospitals and managed care organizations), and support (e.g., laboratories and pharmacies) health care services.[13] Health care payers and providers were disclosing data for public (e.g., public health) and commercial (e.g., marketing) purposes. To create more efficient methods of storage and dissemination of health data, government and the private sector developed more sophisticated information systems, including electronic databases.[14] The proliferation of health data and the creation of automated data systems heightened patient concerns about loss of privacy. For example, in one poll 88% of adults opposed keeping medical records in a national computerized database.[15] Many people worried about unauthorized disclosures of information and breaches of security—e.g., electronic piracy where hackers gain access to electronic health databases.[16] The national health data privacy regulations responded to these privacy concerns and focused on the goal of enhanced personal autonomy.[17]

The national privacy rules, however, failed to pay sufficient attention to the many advantages of systematic collection and use of electronic health data. More accurate and accessible

13. *See* Lawrence O. Gostin, *Personal Privacy in the Health Care System: Employer-Sponsored Insurance, Managed Care, and Integrated Delivery Systems*, 7 KENNEDY INST. ETHICS J. 361, 364 (1997).

14. *See* COMM. ON MAINTAINING PRIVACY AND SEC. IN HEALTH CARE APPLICATIONS OF THE NAT'L INFO. INFRASTRUCTURE, NAT'L RESEARCH COUNCIL, FOR THE RECORD: PROTECTING ELECTRONIC HEALTH INFORMATION 21-22 (1997).

15. INST. FOR HEALTH FREEDOM, *supra* note 7, at 3

16. *See* California HealthCare Foundation, *Americans Worry About the Privacy of Their Computerized Records* (Jan. 28, 1999), *available at* http://www.chcf.org/press/view.cfm?itemID=12267.

17. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,461 (Dec. 28, 2000) ("These protections will begin to address growing public concerns that advances in electronic technology and evolution in the health care industry are resulting, or may result, in a substantial erosion of the privacy surrounding individually identifiable health information maintained by health care providers, health plans and their administrative contractors."), *available at* http://aspe.hhs.gov/admnsimp/final/PvcPre01.htm.

data allow patients to make more informed decisions about health plans, providers, products, and health care charges. Data improve clinical care by assisting physicians in decision making (e.g., faster and more accurate diagnoses),[18] providing increased oversight (e.g., reduction of medical errors[19] and adverse drug events),[20] and disseminating expert medical information in traditionally under-served communities (e.g., telemedicine). Society benefits as well. Efficient data systems facilitate research on the causes of injury and disease, effective interventions (e.g., vaccines and pharmaceuticals), and the quality and cost-effectiveness of health services. Data systems also improve public health surveillance[21] and response to infectious diseases and other threats to the population.[22] Electronic information systems not only improve health care and achieve public benefits, but also offer better data security. Electronic tools such as personal access codes, encryption,[23] and audit trails[24] can more efficiently prevent and detect unauthorized access to data systems.[25]

A. TRADITIONAL BALANCING OF INDIVIDUAL AND COLLECTIVE INTERESTS: THE SALIENCE OF AUTONOMY

The achievement of these, and other, public goods comes with a cost. Whenever data are shared without the person's

18. *See* Dereck L. Hunt et al., *Effects of Computer-Based Clinical Decision Support Systems on Physician Performance and Patient Outcomes*, 280 JAMA 1339 (1998).

19. *See* David W. Bates et al., *Effect of Computerized Physician Order Entry and a Team Intervention on Prevention of Serious Medication Errors*, 280 JAMA 1311 (1998); Nicolas P. Terry, *An eHealth Diptych: The Impact of Privacy Regulation on Medical Error and Malpractice Litigation*, 27 AM. J.L. & MED. 361 (2001).

20. *See* Robert A. Raschke et al., *A Computer Alert System to Prevent Injury from Adverse Drug Events*, 280 JAMA 1317 (1998).

21. *See* Lawrence O. Gostin et al., *The Public Health Information Infrastructure: A National Review of the Law on Health Information Privacy*, 275 JAMA 1921, 1921 (1996); *see also* Antoine Flahault et al., *FluNet as a Tool for Global Monitoring of Influenza on the Web*, 280 JAMA 1330 (1998) (describing an Internet application developed by the World Health Organization to monitor the influenza virus globally).

22. *See, e.g.*, LAWRENCE O. GOSTIN, PUBLIC HEALTH LAW: POWER, DUTY, RESTRAINT 113-25 (2000).

23. *See* Elizabeth Corcoran, *Breakthrough Possible in Battle Over Encryption Technology*, WASH. POST, July 12, 1998, at A8.

24. *See* SYS. SEC. STUDY COMM., NAT'L RESEARCH COUNCIL, COMPUTERS AT RISK: SAFE COMPUTING IN THE INFORMATION AGE 88 (1991).

25. *See* Gostin, *supra* note 4, at 492-93.

express agreement there is a loss of autonomy. Whenever intimate data are seen by family or friends there may be a feeling of embarrassment. Whenever data are seen by employers or insurers there is the potential for discrimination.

There are good reasons for the concern about personal privacy. Health data contain highly sensitive information such as diagnoses, treatments, disabilities, and clinical histories. Some of this information is particularly sensitive, such as HIV/AIDS or other sexually transmitted infections, mental health, alcohol or drug use, reproductive status, and genetic diagnoses. Medical records also contain non-health related personal information that can be used to create a broader profile of the individual's lifestyle and behaviors, including (1) personal identifiers (e.g., Social Security number, addresses, phone numbers, and place of employment); (2) demographics (e.g., age, sex, race, marital status, and children); (3) finances (e.g., employment and insurance status, income, and methods of payment); (4) information about why treatment is sought (e.g., the victim of a violent crime, firearm injury, workplace accident, or the at-fault party in an auto accident); and (5) confidential expressions of patient concerns about her condition.[26]

It would be convenient to think that society could achieve individual interests in privacy and collective interests in research, public health, or other common goods. Indeed, in some senses privacy protection can promote public goods by facilitating the doctor/patient relationship and encouraging individuals to fully utilize health services, cooperate with health agencies, and avoid falsification of their medical records.[27] But more often than not, strict privacy rules dilute public benefits. Consider a privacy rule that invariably defends personal choice with respect to disclosures for research or public health. Not everyone will willingly permit the sharing of personal medical information for these, or other, public purposes. It might be argued that it is all right if some people refuse, provided most agree to share their data. However, the simple acts of asking and permitting individuals full control over their data can defeat the achievement of the public objective. For example, if people can opt out of health services research, there will be a

26. *See* Lawrence O. Gostin, *Health Care Information and the Protection of Personal Privacy: Ethical and Legal Considerations,* 127 ANNALS INTERNAL MED. 683, 684 (1997).

27. *See* Hodge, Gostin & Jacobson, *supra* note 8, at 1470.

self-selection bias that seriously compromises the study.[28] If individuals can refuse to allow their data about infectious diseases, gunshot wounds, or other reportable conditions to be sent to state public health authorities, surveillance would be seriously undermined.

Given the tradeoffs between privacy and the common good, it is necessary to have rules for balancing these potentially competing interests. The extant scholarship tends to offer either a rigorous defense of privacy[29] or an expansive defense of public goods.[30] Scholars rarely provide a framework for balancing with reasons for choosing one good over the other. More often than not, policymakers attempt to reach a balance through an *ad hoc* consideration of several factors. How sensitive is the health data to be protected? What are the interests of the individual in maintaining the privacy of the data versus allowing its disclosure? What are the interests of data holders in protecting the privacy of the data? Are the data traditionally shared for communal purposes? Do the entities that use data for communal purposes typically respect the privacy of the data for its intended uses?

In the section below, we discuss the most traditional method of balancing private and collective interests—that is, by declaring the salience of autonomy. We then offer a new framework for balancing individual interests in privacy with societal interests in sharing the data for justifiable public purposes.

1. The Salience of Personal Autonomy

In an American society that strongly values personal autonomy and decisionmaking,[31] protecting individual privacy is often seen as an overriding objective.[32] This is particularly

28. Lawrence O. Gostin & Jack Hadley, *Health Services Research: Public Benefits, Personal Privacy, and Proprietary Interests*, 129 ANNALS INTERNAL MED. 833, 834 (1998).

29. *See, e.g.*, JOY PRITTS ET AL., THE STATE OF HEALTH PRIVACY: AN UNEVEN TERRAIN (1999), *available at* http://www.georgetown.edu/research/ihcrp/privacy/statereport.pdf.

30. *See, e.g.*, AMITAI ETZIONI, THE LIMITS OF PRIVACY (1999).

31. *See Domestic and International Data Protection Issues: Hearing Before the Subcomm. on Gov't Info., Justice, and Agric. of the House Comm. on Gov't Operations*, 102d Cong. 1-2 (1991); ALAN WESTIN ET AL., THE EQUIFAX REPORT ON CONSUMERS IN THE INFORMATION AGE (1990).

32. *See* Paul Starr, *Health and the Right to Privacy*, 25 AM. J.L. & MED. 193, 194 (1999).

true in the field of health informational privacy.[33] Bioethicists, legal scholars, advocates, and the media have extolled the virtues of health informational privacy.[34]

Ethical justifications for privacy frequently begin with the ancient Hippocratic Oath that admonishes physicians to disclose personal information.[35] If the Hippocratic Oath has any modern moral force, it would apply principally to physicians engaged in a therapeutic relationship. The Oath is directed to the physician and instructs her to keep patient confidences secret. However, most health data are not directly disclosed by patients or held by treating physicians. Rather, data are generated from multiple sources such as laboratories, pharmacies, and research. Data are also used by many entities such as employers, insurers, and managed care organizations. In a complex modern world, data cannot be maintained tightly within the bounds of a single physician/patient relationship.

Modern bioethicists defend health informational privacy on grounds of respect for persons. According to this reasoning, competent adults have full moral authority to make their own decisions about their physical and mental well-being.[36] Privacy enhances individual autonomy by allowing individuals control over identifiable health information. By exercising control, individuals can limit disclosures to persons of their choosing. Controlling their personal information can help individuals pursue their life goals without outside interference.

Ethicists also use utilitarian arguments to defend privacy. Medical confidentiality facilitates intimate relationships between a doctor and her patient, or a health researcher and his subject. This allows patients to feel comfortable divulging personal information that is often needed for accurate diagnoses and treatment. As explained above, unauthorized uses or disclosures may subject individuals to embarrassment, social stigma, and discrimination.[37]

---

33. *See* Jennifer Kulynych & David Korn, *The Effect of the New Federal Medical-Privacy Rule on Research*, 346 NEW ENG. J. MED. 201, 201 (2002).

34. *See, e.g.*, Charity Scott, *Is Too Much Privacy Bad For Your Health? An Introduction to the Law, Ethics, and HIPAA Rule on Medical Privacy*, 17 GA. ST. U. L. REV. 481 (2000).

35. *See* Welch, *supra* note 5, at 371.

36. *See* TOM L. BEAUCHAMP & JAMES F. CHILDRESS, PRINCIPLES OF BIOMEDICAL ETHICS 126 (4th ed. 1994).

37. *See, e.g.*, Madison Powers, *Privacy and the Control of Genetic Information, in* THE GENETIC FRONTIER: ETHICS, LAW, AND POLICY 77, 80 (Mark S. Frankel & Albert H. Teich eds., 1994); Gostin & Hodge, *supra* note 9, at 724.

These, and other, philosophical arguments favoring privacy are valid and important. However, they do not mean that privacy should be absolute or that autonomy should always prevail. Privacy may need to give way if necessary to promote certain public goods. Most liberal conceptions of liberty recognize, for example, that personal autonomy may not be used to cause significant harm to others.[38] Thus, physicians may have a duty to warn third parties of significant risk of violence[39] or infectious disease.[40]

Policymakers have responded to public concerns about privacy by enacting laws[41] that tend to accentuate the value of autonomy. Individuals are often granted significant levels of control over how their health data are accessed, used, and disclosed. For example, health information privacy laws, including DHHS's privacy regulations, typically feature an "anti-disclosure rule." That is, disclosures of identifiable health information are prohibited without the individual's informed consent, subject to some exceptions. This anti-disclosure rule can thwart legitimate exchanges of health data for communal purposes. Under this simplistic formulation, enhancing individual autonomy becomes a means for limiting the exchange of information irrespective of the good to be achieved. This can lead to reduced cost-effectiveness in clinical care, research, public health, and other areas of public need.

2. Communal Uses of Identifiable Health Data

The focus on privacy in scholarship and policymaking fails to give sufficient weight to data uses for improving health, safety, and security. Thoughtful uses of health data can reduce health care costs, facilitate research, advance the public's health, and achieve many other benefits. Just as individuals may have an interest in autonomy, so too do they have an interest in living in a healthier, more secure society. Consider just some of the ways in which data sharing can improve social well-being.

38. *See* BEAUCHAMP & CHILDRESS, *supra* note 36, at 126.

39. Tarasoff v. Regents of the Univ. of Cal., 551 P.2d 334 (Cal. 1976).

40. *See, e.g.*, Hofmann v. Blackmon, 241 So. 2d 752, 753 (Fla. Dist. Ct. App. 1970).

41. *See, e.g.*, PRITTS ET AL., *supra* note 29.

Reducing Costs by Improving Administrative Efficiency

In the United States, health care costs are reimbursed using a complex array of private (e.g., risk retention plans and health insurance) and public (e.g., Medicaid and Medicare) sources of finance. Manual billing for health care, and other administrative costs, is inefficient and expensive. Computerizing health data in an electronic health information infrastructure can reduce these costs by (1) creating databases containing enrollment, financial, and utilization data, and (2) facilitating payment and reimbursement transactions between health providers and insurance plans. DHHS estimates that the use of electronic health data interchange on a system-wide level will result in $29.9 billion in savings over the next decade.[42] Automation can also reduce fraud and abuse by carefully tracking providers' reimbursement claims and matching those claims with electronic treatment records.[43] To effectuate these savings, national privacy policies should encourage consumer and provider participation in electronic filing techniques, and avoid measures that would limit potential savings (e.g., privacy protections that allow consumers to "opt out" of computerized health databases).[44]

Facilitating Medical and Health Services Research

Medical research on the determinants, prevalence, prevention, and treatment of injury and disease advances clinical and public health.[45] Expansive health care databases can facilitate retrospective studies that rely on existing health data and often involve rigorous design and statistical methods.[46] The sharing

42. U.S. DEP'T OF HEALTH AND HUMAN SERVS., HHS FACT SHEET: PROTECTING THE PRIVACY OF PATIENTS' HEALTH INFORMATION (May 9, 2001), *available at* http://www.aspe.hhs.gov/admnsimp/final/pvcfact2.htm [hereinafter HHS FACT SHEET].

43. *See* COMM. ON REG'L HEALTH DATA NETWORKS, INST. OF MED., HEALTH DATA IN THE INFORMATION AGE: USE, DISCLOSURE, AND PRIVACY 76 (Molla S. Donaldson & Kathleen N. Lohr eds., 1994).

44. *Id.*

45. *See* William L. Roper et al., *Effectiveness in Health Care: An Initiative to Evaluate and Improve Medical Practice*, 319 NEW ENG. J. MED. 1197, 1197 (1988).

46. COMM. ON REG'L HEALTH DATA NETWORKS, INST. OF MED., *supra* note 43, at 72-73 (citing C. Fleming et al., *A Decision Analysis of Alternative Treatment Strategies for Clinically Localized Prostate Cancer*, 269 JAMA 2650 (1993); Grace L. Lu-Yao et al., *An Assessment of Radical Prostatectomy: Time Trends, Geographic Variation, and Outcomes*, 269 JAMA 2633 (1993)).

of health data facilitates classic randomized, controlled trials, particularly large-scale clinical trials that study the safety and efficacy of pharmaceuticals and vaccines. Health services research includes the investigation of clinical decisions made by health care professionals, health services or patterns of practice, behavioral changes of individuals and populations, and the distribution and determination of health-related states or events in specified populations.[47] Assessing the quality of health services requires the free exchange of enormous amounts of health information, including data related to (1) access to care (e.g., waiting times to see primary care practitioners and specialists); (2) appropriateness of care (e.g., numbers and severity of adverse events based on comparisons among regional practices or guidelines); (3) health outcomes (e.g., percentage of low birth weight infants, or mortality rates after a heart attack or stroke); (4) health promotion (e.g., education programs such as smoking cessation or stress management classes); (5) disease prevention (e.g., rates for vaccinations, mammograms, prenatal care, or HIV screening); and (6) overall satisfaction with care (e.g., percentage of enrollees satisfied with the plan or satisfied with their primary care physician, percentage of enrollees leaving the plan, and the number of complaints filed).

Modern privacy protections, however, can threaten the accuracy and use of health information for medical research. Privacy protections that allow consumers to restrict the flow of their data through informed consent or advance authorization requirements may hinder the collection of comprehensive and accurate information that may benefit health consumers.[48] Congress and some states legislatures, for example, have attempted to protect the privacy of genetic information by giving individuals proprietary interests in their genetic information.[49] Vested with data property rights, individuals can exert significant control over how such information is used, including for the purposes of medical research. Other privacy laws, including DHHS's health information privacy regulations, require

47. *See* John M. Last, *Epidemiology and Ethics*, 19 LAW, MED. & HEALTH CARE 166, 166-68 (1991).

48. *See* Douglas Sharrott, *Provider-Specific Quality-of-Care Data: A Proposal for Limited Mandatory Disclosure*, 58 BROOK. L. REV. 85, 89-92 (1992).

49. LAWRENCE O. GOSTIN ET AL., NATIONAL CONFERENCE OF STATE LEGISLATURES, GENETICS POLICY AND LAW: A REPORT FOR POLICYMAKERS (2001).

specific informed consent of subjects in many research applications. The additional expenses of conducting medical research entailed in informed consent legislation can stymie health research and may offer few benefits for patients. Responding to public pressure for rigorous privacy protection, Minnesota enacted legislation that restricts access to medical records for research purposes. The law requires advance, written informed consent of patients for health records to be used for medical research. After implementing the law, the Mayo Clinic in Rochester, Minnesota reported that 96% of patients contacted for the purposes of obtaining informed consent agreed to allow their medical information to be released to researchers. This response rate reflects the strong willingness of those receiving medical care to allow their information to be used for medical research, but comes at significant expense to medical researchers.[50] As explained previously, even if most patients can be tracked and acquiesce to participating in health services research, the data may be scientifically skewed due to self-selection biases.

Safeguarding the Public Health

Tracking disease and injury in the population and providing well-targeted prevention services can reduce public health threats more effectively and at significantly less expense than personal medical services.[51] Public health agencies at the federal, state, tribal, and local levels of government have strong demands for extensive access to identifiable health data.[52] This information is the lifeblood of public health practice. When aggregated, health data can help monitor the incidence, patterns, and trends of injury and disease in populations.[53] Carefully planned surveillance or epidemiological studies facilitate rapid identification of health needs, including (1) the spread of communicable or sexually transmitted infection or disease (e.g., HIV, TB, hepatitis B virus); (2) clusters or outbreaks of bacte-

50. L. Joseph Melton, III, *The Threat to Medical-Records Research*, 337 NEW ENG. J. MED. 1466, 1467 (1997).

51. U.S. DEP'T OF HEALTH & HUMAN SERVS., HEALTHY PEOPLE 2000: NATIONAL HEALTH PROMOTION AND DISEASE PREVENTION OBJECTIVES (1991); Lawrence O. Gostin, *Securing Health or Just Health Care? The Effect of the Health Care System on the Health of America*, 39 ST. LOUIS U. L.J. 7, 12-14 (1994).

52. *See* COMM. FOR THE STUDY OF THE FUTURE OF PUB. HEALTH, INST. OF MED., THE FUTURE OF PUBLIC HEALTH app. A (1988).

53. Gostin & Hodge, *supra* note 9, at 710-14.

rial or viral infection (e.g., Legionnaire's disease, hanta virus, E. Coli) from naturally occurring sources or bioterrorism; (3) risk behaviors in sub-populations (e.g., smoking among female adolescents or ethnic minorities); and (4) harmful conditions (e.g., child or spousal abuse, lead poisoning, radon, iatrogenic injuries, or gunshot wounds). Tracking health risks allows public health authorities to allocate resources and interventions to areas of greatest need.

As with medical and health services research, privacy protections may limit public health authorities' access to needed data. Many state laws are so focused on privacy that they hinder or prevent basic exchanges of information within the public and private health sectors. Public health authorities may not be able to share relevant data with law enforcement or emergency management agencies even in the event of bioterrorism.[54] Additionally, public health authorities may not be permitted to monitor health care data in hospitals, managed care organizations, and pharmacies, even though these data may provide an early warning of an infectious disease outbreak or bioterrorism.[55] In these ways, privacy regulations are used as a shield to prevent public and private sharing of health data for the public's health and security.

Existing privacy laws may also prevent public health authorities from sharing data with each other. Registries of data concerning contagious diseases (e.g., tuberculosis) or other conditions (e.g., cancer) may not be shared among public health authorities due to specific privacy protections for certain types of information. Some states do not expressly permit disclosure of public health information to other states for the control of communicable diseases.[56] As a result, persons with HIV infection, sexually transmitted diseases, or tuberculosis may be lost to follow-up when they move from state to state, or different parts of the same state, due to prohibitions against releasing identifiable health information.[57] State public health authorities may refuse as well to distribute public health information to federal public health authorities on grounds that the infor-

54. Lawrence O. Gostin, *Conceptualizing the Field After September 11th: Foreword to a Symposium on Public Health Law*, KY. L.J. (forthcoming 2002).

55. *See* Rene Bowser & Lawrence O. Gostin, *Managed Care and the Health of a Nation*, 72 S. CAL. L. REV. 1209, 1217-18 (1999).

56. Gostin et al., *supra* note 21, at 1925 (e.g., Arkansas, Indiana, and West Virginia).

57. *Id.*

mation is protected against disclosure by privacy laws. The Centers for Disease Control and Prevention (CDC), for example, has had requests for cancer-related data rebuffed by state public health authorities who hold such data. CDC needs these data for national public health research. Some state registries, however, refuse to supply it, citing privacy-specific laws and regulations that only allow the release of data to specified entities, like the National Cancer Institute, or in a non-identifiable format.

B. MAXIMIZING INDIVIDUAL AND COMMUNAL INTERESTS

Balancing individual and collective interests in privacy and data sharing is complex. Rather than conceiving individual autonomy as a dominating factor in balancing, we propose a different approach. Our framework for balancing values individual privacy and common goods, without *a priori* favoring either. National health information privacy policies can maximize privacy interests where they matter most to individuals and maximize communal interests where they are likely to achieve the most public good. Our framework focuses on the nature and extent of the potential harms to individuals and the goods that can be achieved from data disclosures.

This theoretical structure may be criticized on the grounds that it is overtly utilitarian and fails to give sufficient weight to the norm of respect for persons. Seen in the context of modern liberalism, a framework that does not offer individuals full control over uses of personal data is vulnerable to a harsh critique. Modern liberalism frequently sees individuals as isolated beings devoid of social context. But people live in networks of families, neighborhoods, towns, and cities. The norm of respect for persons assumes that maximizing each individual's freedom will benefit society as well. Giving each person a veto over participation in activities that provide manifest social advantages is not beneficial to the wider community. It means that a few individuals can hinder activities that enhance well-being for the population. Individuals may desire privacy, but they should also want to live in communities that promote health, safeguard security, and facilitate medical research.

Finding a balance between individual choice and public goods requires an assessment of consequences and, therefore, is frankly utilitarian. Some questions cannot be avoided: How much do individuals lose by giving up some control over personal information? How much does society gain by the freer

use of health information? It is important to see that trade-offs between private and public interests are necessary. Only in this way is it possible to give individuals a certain level of privacy without jeopardizing all the good that can come from information collection and dissemination.

Uses or Disclosures for the Common Good.

Where 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 (e.g., cost-effective health care, public health, and research). In such cases, public entities should be able to acquire and use the data regardless of individual informed consent or other privacy protections. Nor should privacy standards or procedures be so inflexible (e.g., property rights in health data) or expensive (e.g., specific informed consent for use of health data in medical research) that they significantly impede the achievement of common goods.

Consider a rule that provides flexibility in the use of health data for legitimate health care, public health, or research purposes. We are making the assumption that data users are likely to achieve an important public purpose and will not disclose information outside the health care, public health, or research enterprise in which they are engaged. In such circumstances individuals are unlikely to experience intangible harm such as embarrassment or more tangible damage such as discrimination. Health care providers, public health officials, or researchers usually do not seek or use information in ways that are detrimental to the individual. Data disclosures outside the public enterprise (e.g., to the patient or subject's family, friends, or employer) would be subject to strict privacy rules.

Although use of health data for important public purposes would be permitted under our standards, data users would still be required to demonstrate the public need and limit the potential for individual harm. The following principles would apply to all data users: (1) demonstrate the need for data to achieve an important public purpose; (2) demonstrate that the data sought are the least extensive necessary to achieve the public purposes; (3) de-identify the data whenever possible and practicable, consistent with the achievement of the public good; (4) implement privacy and security standards to ensure that persons may access data only where necessary for the performance of essential functions; and (5) implement fair information prac-

tices such as permitting individuals access to their health information and the purposes for which it is being used. Provided these measures are observed, a regular and free exchange of data should occur.

Uses or Disclosures Likely to Result in Harm

Where identifiable health data are used or disclosed in ways that are not likely to achieve an important public benefit, and the risks to individuals are high, privacy safeguards should be robust. In such cases, standards and procedures for safeguarding privacy, such as informed consent and anti-disclosure prohibitions, are appropriate. For example, if a health care or public health professional discloses intimate personal information to friends, neighbors, employers, or insurers, the potential harm of embarrassment, stigma, or discrimination is high, but public benefits are low. Imposing a rule that data cannot be used outside the health care, public health, or research system does not significantly jeopardize the achievement of public goods, and reassures patients that disclosures likely to cause them harm will not occur.

This framework for balancing will not prevent some patients from feeling wronged when personal information is used in ways of which they do not approve. Even if they are not harmed in discrete ways, patients may feel aggrieved by the failure to respect their choices. This feeling of personal entitlement is fostered by a culture that celebrates individual autonomy and de-emphasizes collective well-being. A cultural expectation, supported by a legal rule, that asks each individual to give up a small amount of autonomy in exchange for substantial benefits for the community may change patient expectations and result in a healthier society. Our framework is based on a common sense understanding that individual interests should yield if personal burdens are small and potential public benefits are substantial.

II. THE NATIONAL HEALTH INFORMATION PRIVACY STANDARD

To be effective, a comprehensive, national health information privacy policy should balance individual interests in protecting the privacy of health data with societal needs to share the data for communal purposes.[58] Reaching this balance on a

58. *See* Donna E. Shalala, *Health Care Information and Privacy*, 8

national scale has proven to be precarious. In this and the subsequent Part, we briefly describe the process through which national health information privacy regulations came about, the scope of these regulations, and particularly how these regulations fit with our framework for balancing.

A. THE SCOPE OF THE STANDARD

Health information privacy regulations promulgated by DHHS pursuant to congressional authority under HIPAA are the product of years of legislative and administrative efforts. Through HIPAA, Congress originally imposed a deadline of August 21, 1999 to pass health information privacy legislation.[59] As a result of interest group lobbying,[60] a diverse health law and policy agenda, and party politics in the House and Senate, Congress failed to pass a comprehensive privacy law by the deadline.[61] HIPAA authorized the Secretary of DHHS to issue privacy regulations in the event that Congress failed to act within its self-imposed deadline.[62] The initial publication of DHHS's proposed regulations in November 1999[63] garnered over 52,000 public comments[64] and delayed the production of the final regulations until December 2000.[65] After President Bush took office, privacy advocates were concerned that his administration might scale back or eliminate the regulations altogether.[66] On April 14, 2001, however, the regulations were finalized subject to interpretive guidelines,[67] the first of which

---

HEALTH MATRIX 223, 230-31 (1998).

59. HIPAA, Pub. L. No. 104-191, § 264(c)(1), 110 Stat. 1936, 2033 (1997).

60. *See* Amy Goldstein & Robert O'Harrow, *Bush Will Proceed on Patient Privacy*, WASH. POST, Apr. 13, 2001, at A1.

61. *Id.*; *see* HHS FACT SHEET, *supra* note 42.

62. HIPAA § 264(c)(1).

63. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918-60,065 (Nov. 3, 1999).

64. Peter A. Setness, *HIPAA and the Changing Face of Patient Privacy: New Legislation Requires Timely Response*, 111 POSTGRADUATE MED. (2002), *available at* http://www.postgradmed.com/issues/2002/01_02/editorial_jan.htm.

65. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462-829 (Dec. 28, 2000).

66. *See* HEALTH PRIVACY PROJECT, COMMENTS ON THE FINAL FEDERAL STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION 2-3 (2001); Terry, *supra* note 19, at 361; Goldstein & O'Harrow, *supra* note 60; *see also* Robert Pear, *White House Plans to Revise New Medical Privacy Rules*, N.Y. TIMES, Apr. 8, 2001, at 22 (announcing the Bush administration's position to revise the rules).

67. *See* Goldstein & O'Harrow, *supra* note 60; Pear, *supra* note 66.

were released by DHHS in July 2001.[68] The regulations take effect for most covered entities on April 14, 2003, and a year later for small health plans.

Though their development was convoluted, the health data privacy regulations provide privacy protections for health care consumers[69] within the scope of DHHS's limited authority under HIPAA.[70] In this section, we address two questions concerning the national health information privacy regulations: (1) What information is protected? and (2) to whom do the protections apply?

1. What Information is Protected?

The regulations explicitly cover individually identifiable health information[71] (i.e., protected health information (PHI)).[72] PHI includes any data that contains uniquely identifiable characteristics, including a name, social security or drivers' license

68. OFFICE FOR CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVS., STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION, *available at* http://www.aspe.hhs.gov/admnsimp/final/pvcguide1.htm (last revised July 6, 2001) [hereinafter DHHS STANDARDS]; Ceci Connolly, *Guidelines on Patient Privacy Rules Issued*, WASH. POST, July 7, 2001, at A6; Robert Pear, *Administration Clarifies New U.S. Rules Guarding Privacy of Patients*, N.Y. TIMES, July 7, 2001, at A9.

69. To enforce these protections, DHHS's Secretary can investigate complaints and conduct compliance reviews. Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. §§ 160.306, .308 (2001). Violations of the standard can lead to civil and criminal penalties up to $250,000 and ten years in prison. HHS FACT SHEET, *supra* note 42. There is no private right of action for individuals to redress violations.

70. *Cf.* A. Craig Eddy, *A Critical Analysis of Health and Human Services' Proposed Health Privacy Regulations in Light of The Health Insurance Privacy* (sic) *and Accountability Act of 1996*, 9 ANNALS HEALTH L. 1, 50-60 (2000) (discussing the constitutional issues involved in Congress's delegation of authority to DHHS under HIPAA).

71. *Health information* is comprehensively defined as data (1) "created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse;" and (2) "relate[d] to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." 45 C.F.R. § 160.103 (2001) (defining "health information").

72. *Id.* § 164.514. DHHS defines individually identifiable health information as health information that "identifies [an] individual" or "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." *Id.* § 164.501 (defining "individually identifiable health information"). The regulatory definition limits the term to only a subset of health information, specifically that created or received by health care providers, health plans, employers, or health care clearinghouses. *Id.*

number, address, fingerprint, or genetic link.[73] Where health data are truly non-identifiable, privacy interests are minimal.[74] Consequently, the national privacy rules do not restrict access, use, or disclosure of non-identifiable data. Non-identifiable data (e.g., aggregate statistical data, non-linked data, or other data stripped of all individual identifiers) thus require no individual privacy protections,[75] and are not covered by the regulations. This provides an incentive for data holders to use or de-identify health information to diminish the risk of harmful disclosures and uses of personal data.[76] DHHS permits covered entities to de-identify by assigning codes that can later allow for re-identification.[77]

PHI includes all mediums (electronic, oral, and paper) of health information.[78] Protecting the privacy of all mediums of health information recognizes the impracticability of separating paper-based records from electronic or oral-based data. Failing to protect all mediums of health data would leave a sig-

---

73. The health data privacy rule outlines two means for determining if health information is not individually identifiable, or "de-identified," and thus no longer regulated by the rule. First, an expert utilizing accepted analytic techniques can conclude that "the risk is very small that the information could be used, alone or in combination with other reasonably available information" to identify the subject of the information. *Id.* § 164.514(b)(1)(i). A second permitted means of de-identification is that the covered entity can remove a comprehensive set of identifiers of the individual and of relatives, employers, and household members of the individual. These identifiers include names, geographic subdivisions smaller than a state, dates more specific than years, contact information such as telephone and fax numbers and e-mail addresses, identification numbers such as social security numbers, account and medical record numbers, license place numbers, etc.; and full face photographic images. *Id.* § 164.514(b)(2)(i).

74. *Contra* Yaron F. Dunkel, *Medical Privacy Rights in Anonymous Data: Discussion of Rights in the United Kingdom and the United States in Light of the* Source Informatics *Cases*, 23 LOY. L.A. INT'L & COMP. L. REV. 41 (2001).

75. Non-identifiable health data may raise privacy concerns at a group level, although DHHS's regulations do not attempt to address or protect "group privacy" interests. For a definition of "group privacy" in the context of genetic data, see James G. Hodge, Jr. & Mark E. Harris, *International Genetics Research and Issues of Group Privacy*, J. BIOLAW & BUS., Special Supp. 15 (2001).

76. *See* HEALTH PRIVACY PROJECT, BEST PRINCIPLES FOR HEALTH PRIVACY 15-16 (1999).

77. The code must not be derived from or related to information about the individual or able to be translated so that the individual can be identified. 45 C.F.R. § 164.514(c)(1) (2001). The covered entity must also not disclose or use the code for other purposes than record identification and cannot disclose the mechanism for re-identification. *Id.* § 164.514(c)(2).

78. *Id.* § 164.501 (defining "protected health information").

nificant amount of health communications unregulated by federal law and complicate enforcement.[79] Through HIPAA, however, Congress may have limited DHHS's authority to regulate non-electronic communication.[80] Although DHHS maintains it has "ample legal authority,"[81] its regulations are structured so that provisions concerning non-electronic communications are severable by court action from electronic communications.[82]

2. Who is Covered?

Congress has limited DHHS's authority to promulgate health information privacy regulations to a defined set of persons.[83] The regulations apply to covered entities (health care plans, health providers, and health care clearinghouses[84]) and

79. *See* PRITTS ET AL., *supra* note 29, at 6-7.

80. Section 264 of HIPAA, which contains the congressional mandate to DHHS to develop the privacy standard, evolved because of the administrative simplification goals of the statute related to electronic information exchange. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,469 (Dec. 28, 2000); *see also* Eddy, *supra* note 70, at 18. The statute describes the scope of DHHS's authority in terms of regulation of individual rights over *individually identifiable health information*, not electronic transactions or administrative simplification. The statute states that if Congress fails to meet the deadline, DHHS must "at least" develop regulations that address "(1) The rights that an individual who is a subject of individually identifiable health information should have (2) The procedures that should be established for the exercise of such rights [and] (3) The uses and disclosures of such information that should be authorized or required." HIPAA, Pub. L. No. 104-191, § 264(b), 110 Stat. 1936 (1997) (giving the requirements for DHHS's recommendation to Congress when Congress is considering legislation before its self-imposed deadline has passed). In a cross-reference to section 264(b), section 264(c) applies these requirements to the regulations that are mandated if Congress doesn't meet its deadline. *Id.* § 264(c), 110 Stat. at 2033. The use of "at least" and the lack of a reference to the administrative simplification sections or electronic transactions in these detailed requirements suggests that Congress did not intend to limit DHHS to protecting privacy in electronic transactions only. PRITTS ET AL., *supra* note 29, at 5.

81. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,496 (Dec. 28, 2000).

82. *Id.* In a successful court challenge to the broad coverage, the judge could order that the phrase "regarding non-electronic information" be struck from the regulation while the standard would remain intact for electronic communications.

83. 45 C.F.R. § 160.102 (2001).

84. A *health care clearinghouse* is

> a public or private entity, including a billing service, repricing company, community health management information system or community health information system . . . that . . . (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into

their business associates. Health plans, which provide or pay for the cost of medical care, are covered whether they are private entities (e.g., health insurers or managed care organizations) or government organizations (e.g., Medicaid, Medicare, or the Veterans Administration).[85] Health care providers (e.g., physicians, hospitals, and clinics) are covered if they "transmit[] any health information in electronic form in connection with a transaction covered by [the regulations]."[86] Electronic exchanges can include billing and fund transfers in addition to communications containing health information.

The regulation also applies to the business associates[87] (e.g., lawyers, accountants, billing companies, and other contractors) whose relationships with covered entities require the sharing of PHI.[88] DHHS requires covered entities to assure that their business associates comply with privacy standards.[89] If a covered entity knows of a privacy violation by a business associate and does not address it, the entity may be considered to be violating the rules.[90] Through this oversight function, DHHS regulates some of the downstream users and processors of PHI.[91]

---

standard data elements or a standard transaction [or] (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Id. § 160.103.

85. *Id.* (defining "health plan").

86. *Id.* § 160.102(a)(3).

87. A *business associate* with respect to a covered entity is

a person who . . . assists in the performance of . . . [a] function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or . . . [p]rovides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in section 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

Id. § 160.103.

88. *Id.* § 160.102(a)(3).

89. *Id.* § 164.502(e)(1)(i).

90. *Id.* § 164.502(e)(1)(iii).

91. *See* Lawrence O. Gostin, *National Health Information Privacy: Regu-*

Though the regulations are comprehensive in their coverage, not all persons or entities who regularly use, disclose, or store identifiable health data are covered. The regulations do not cover groups such as auto, life, and worker compensation insurers, even though these entities regularly use personal medical information.[92] Additional protections governing all identifiable health data, regardless of its holder or manner of communication, would broaden national protections of health information privacy.

B. FAIR INFORMATION PRACTICES

Persons and entities maintaining PHI must comply with a range of fair information practices that allows individuals to make informed choices about the delivery and financing of their health care. The health information privacy regulations vest health consumers with several fair information practices, including rights to access protected health information, amend protected health information, receive notice, and request an accounting of disclosures.

1. Access to Protected Health Information

Individuals are granted a range of access rights to their PHI.[93] These include on-site inspections of records and the provision of copies.[94] Covered entities must act within thirty days upon a request for access to health data by a person who is the subject of the data.[95] In most instances, covered entities must accommodate a request for access, or provide a fair and informed process in case of denials.[96] The regulations permit

lations Under the Health Insurance Portability and Accountability Act, 285 JAMA 3015, 3016 (2001).

92. *See* James G. Hodge, Jr., *The Intersection of Federal Health Information Privacy and State Administrative Law: The Protection of Individual Health Data and Workers' Compensation*, 51 ADMIN. L. REV. 117, 118 (1999).

93. 45 C.F.R. § 164.524 (2001). The covered entity may require that the request be in writing. *Id.* § 164.524(b)(1).

94. *Id.* § 164.524(c)(1).

95. *Id.* § 164.524(b)(2)(i). Sixty days is allowed if the information is held off-site. *Id.* § 164.524(b)(2)(ii). Delay is also allowed if the covered entity informs the individual in writing of the reasons it requires more time and when the request will be granted. *Id.* § 164.524(b)(2)(iii).

96. The denial must be in writing and in plain language. It must explain the reasons for the denial, any rights for review over the decision, and methods of complaint to the covered entity. *Id.* § 164.524(d)(2). Access should be granted to any information that does not meet the specific grounds for denial. *Id.* § 164.524(d)(1). If a review of the denial is warranted, it is conducted by a

narrow, unreviewable reasons for denials regarding requests for psychotherapy notes; information likely to be used in a civil, criminal, or administrative proceeding; and requests by inmates to their correctional facility or health care provider that might threaten the health or safety of the individual or others.[97] In limited other circumstances,[98] a covered entity may deny access although an individual may request a review of the grounds for denial.[99] Covered entities may also provide a summary of an individual's PHI instead of the actual documents (if the individual agrees).[100]

2. Amend Protected Health Information

Individuals can amend inaccuracies or missing information in their PHI.[101] The covered entity must act within sixty days on a request to amend.[102] If the covered entity agrees to the amendment, it must (1) identify the records that are affected; (2) append or provide a link to the amendment;[103] (3) inform the individual that the amendment has been made;[104] and (4) work with other covered entities or business associates who possess or receive the data to make the amendments as well.[105] As

licensed health care professional who is designated by the covered entity but is not directly involved in the decision to deny access. *Id.* § 164.524(d)(4).

97. *Id.* § 164.524(a)(1), (2). Information obtained from another based on a promise of confidentiality that would likely reveal the identity of the source may be denied without review. *Id.* § 164.524(a)(2)(v). Also, health care providers may temporarily deny access during research based on an individual's care if the individual has consented to both the research and the denial of access during research. *Id.* § 164.524(a)(2)(iii).

98. *Id.* § 164.524(a). These situations include where a licensed health care professional determines that access will endanger the life or physical safety of the individual or another person. *Id.* § 164.524(a)(3)(i).

99. *Id.* § 164.524(a)(4). This provision specifically covers determinations that references to another person will endanger that other individual. *Id.* § 164.524(a)(3)(ii). It also covers situations in which the access is "reasonably likely to cause substantial harm to the individual or another person." *Id.* § 164.524(a)(3)(iii).

100. *Id.* § 164.524(c)(2)(ii).

101. *Id.* § 164.526.

102. *Id.* § 164.526(b)(2)(i). An extension of thirty days is possible if the covered entity explains the reasons for delay and the date on which it will respond to the request in writing to the individual. *Id.* § 164.526(b)(2)(ii).

103. *Id.* § 164.526(c)(1).

104. *Id.* § 164.526(c)(2), (3). It must also notify persons or entities (1) identified by the individual as needing the amended information; or (2) known by the covered entity to have PHI about the individual and who may rely on the information to the detriment of the individual. *Id.*

105. *Id.* § 164.526(e).

with access rights, covered entities may deny amendments in certain circumstances, particularly if they determine that the record is "accurate and complete,"[106] with written notice to the individual.[107] Unlike disputes over denial to access, there is no final review to clarify which party, the individual or the covered entity, is correct. A covered entity may merely respond to individual disagreements with a written rebuttal.[108]

3. Receive Notice

HIPAA provides that "[i]ndividuals ha[ve] the right to adequate notice of the uses and disclosures of [PHI] that may be made by the covered entity,"[109] and to know the covered entity's privacy and security policies and fair information practices requirements.[110] Notices must be in plain language to avoid confusion.[111] The timing of the notice required depends on the type of covered entity.[112] Additional consumer safeguards apply to

106. *Id.* § 164.526(a)(2)(iv). Other grounds for denial are (1) if the covered entity did not create the information or record, it may deny the request unless the individual reasonably shows that the originator of the information is no longer available to address the amendment request and (2) if the individual could not access the record because of restrictions laid out in section above, the covered entity would have grounds to deny the amendment. *Id.* § 164.526(a)(2)(i), (iii).

107. *Id.* § 164.526(d)(1). It must be in plain language and explain the reasons for the denial, any rights for review of the decision, and methods of complaint to the covered entity. *Id.*

108. *Id.* § 164.526(d)(3). The individual must be provided with a copy of the rebuttal. The written statement and rebuttal must then be appended or linked to the appropriate records by the covered entity, *id.* § 164.526(d)(4), and included, when relevant, in any future disclosures. *Id.* § 164.526(d)(5)(i). "If the individual has not submitted a written statement of disagreement," then the request for amendment and the covered entity's denial must be included if the individual has requested such disclosure. *Id.* § 164.526(d)(5)(ii).

109. *Id.* § 164.520(a)(1).

110. *Id.* § 164.520(a)(1). The notice must include information about how individuals may complain about potential misuses or violations to the covered entity and the Secretary of DHHS or contact the covered entity with questions. *Id.* § 164.520(b)(1)(vi).

111. *Id.* § 164.520(b)(1).

112. *Id.* § 164.520(c)(1), (2). Health plans must provide notice to covered individuals by the compliance date of the regulation. *Id.* § 164.520(c)(1)(A). New enrollees must get the notice at time of enrollment. *Id.* § 164.520(c)(1)(B). At least once every three years, the health plan must notify enrollees in the plan that the notice is available and the methods by which they can obtain it. *Id.* § 164.520(c)(1)(C)(ii). In contrast, health care providers have to provide the notice upon the first service delivery after the compliance date. *Id.* § 164.520(c)(2).

covered entities that provide notice electronically.[113]

4. Request an Accounting of Disclosures

Covered entities are required to maintain an accounting of disclosures of PHI (other than for disclosures related to treatment, payment, and health care operations, or other exceptions).[114] The accounting includes the name (and address if known) of the person or entity who received the information, the date of the disclosure, a brief description of the information disclosed, and a brief explanation of the reasons for disclosure if not authorized by the patient.[115] Patients have a limited right to receive the accounting of disclosures over the six year period prior to the request.[116]

C. THE EFFECTS OF PREEMPTION

Pursuant to Congressional mandate through HIPAA, DHHS cannot preempt state health information privacy laws that are more protective of health information privacy rights than the national privacy regulations.[117] Some states may offer more protections through, for example, "super-confidentiality" laws for genetic, mental health, or HIV/AIDS information. Thus, because existing federal or state laws that provide more privacy protections remain, DHHS's privacy regulations create a federal "floor" of protections.

This multi-level approach allows states to tailor health information privacy policies to the specific needs of their popula-

113. *Id.* § 164.520(c)(3). An individual must agree to obtain the notice via e-mail. A paper copy must be provided "if the covered entity knows that the e-mail transmission has failed." *Id.* § 164.520(c)(3)(ii). Health care providers must give electronic notice automatically and simultaneously when their first service delivery is electronic. *Id.* § 164.520(c)(3)(iii). If a covered entity maintains a website that offers information about its benefits and services, it must also prominently post its notice on the website as well as make it available electronically. *Id.* § 164.520(c)(3)(i).

114. *Id.* § 164.528(a)(1). These include disclosures for national security and intelligence purposes; correctional institutions; and health oversight agencies or law enforcement officials who document that the agency's officials would be impeded if the accounting revealed the disclosure. *Id.* § 164.528(a)(1), (2).

115. *Id.* § 164.528(b)(2).

116. *Id.* § 164.528(a)(1).

117. *Id.* § 160.203(b) (2001). State laws are also not preempted if they promote certain goods such as public health, efficacy in payment of health care, fraud prevention, and audits and program monitoring. *Id.* § 160.203(a), (c), (d).

tions, but there are at least two disadvantages (1) Individuals in some states may unfairly benefit from greater privacy protections than in other states; and (2) where most electronic health data are exchanged across state boundaries, covered entities (specifically larger health care providers, plans, and clearinghouses) must adhere to national and regional privacy standards. This results in higher costs than would occur if a uniform national standard were in place.

III. INDIVIDUAL PRIVACY AND SHARING HEALTH DATA

The national privacy regulations restrict the use and disclosure of health data under specified circumstances. Some level of individual control over the use and disclosure of PHI is essential to ensure privacy because of the potential risks of harm from unlimited sharing of personal medical data. The principal question, however, is how much control individuals should exercise. The regulations differentiate among the various purposes for which data may be used and disclosed. Uses and disclosures for health care-related purposes (e.g., provision or payment for health care services) are liberally permitted, albeit with the advance "informed consent" of each patient. Uses and disclosures of PHI for other purposes outside the health care context are limited. Disclosures may be made pursuant to written authorization by the individual who is the subject of the data, subject to some exceptions. In either context, a minimum disclosure rule applies: When using or disclosing PHI, "a covered entity must make reasonable efforts to limit [PHI] to the minimum necessary to accomplish the intended purpose."[118] The minimum disclosure rule helps patients maintain privacy, for example in reimbursement transactions, where only specific health information is needed.[119]

In this Part, we examine DHHS's use and disclosure rules for health care and non-health care purposes and compare

118. *Id.* §164.502(b)(1).

119. DHHS's recent guidance has clarified a significant concern of health care providers over the permitted uses during treatment when consulting with other physicians or medical staff. The standard as written specifies that the minimum disclosure requirement applies for use of PHI during treatment by health care providers, but not disclosures. This has caused confusion about how health care providers can utilize vital health information in the course of treatment as they work with other medical professionals. In the July 2001 guidance, DHHS explained that the exemption for disclosures during treatment allows health care providers to share information with other providers. *See* DHHS STANDARDS, *supra* note 68.

these rules with the balancing framework we have proposed.

A. INDIVIDUAL CONSENT FOR USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION FOR HEALTH CARE PURPOSES

DHHS's regulations presently require covered health care providers to obtain written consent from individuals before using or disclosing information for treatment, payment, or health care operations. Such consent must (1) be in plain language;[120] (2) "[i]nform the individual that [PHI] may be used and disclosed to carry out" those activities;[121] (3) indicate that the individual can revoke the consent in writing;[122] and may (4) request that the covered entity restrict how PHI is used or disclosed for health care purposes (though the covered entity is not required to agree).[123]

Requiring prior informed consent for use and disclosure of health data for transaction purposes is consistent with the prevailing practice in many health care settings in the United States. Most health consumers, often unwittingly, sign a series of waivers upon seeking medical care that allow disclosures among providers, insurers, data handlers, and collection agencies. In a prior version of the health information privacy regulations, DHHS attempted to eliminate the formal informed consent requirement. This was strongly opposed by privacy advocates on the basis that it allowed multiple exchanges of health data without any patient consent. Recently the Bush Administration proposed dropping the informed consent requirement, although no final rule has been made.[124]

The written informed consent requirement for use and disclosure of PHI for health care purposes is poorly designed and ineffective. Consent, in fact, is neither informed nor consensual. A patient is required to sign a consent form on his first visit to a physician; that form provides consent for all future

120. 45 C.F.R. § 164.506(c) (2001).

121. *Id.* § 164.506(c)(1), (2). The consent may not be combined in a single document with the notice. *Id.* § 164.506(b)(3).

122. *Id.* § 164.506(c)(5).

123. *Id.* § 164.506(c)(4). If the covered entity does agree, the agreement is binding. *Id.* § 164.522(a) (restating the standard for an individual's right to request restrictions of uses and disclosures and documenting the requirements for termination of the restrictions).

124. Robert Pear, *Bush Acts to Drop Core Privacy Rule on Medical Data*, N.Y. TIMES, Mar. 22, 2002, *available at* http://www.nytimes.com/2002/03/22/politics/22PRIV.html.

disclosures and uses. At the time the form is signed, the individual is not even aware of the substance of the data protected. The patient may not know what is currently contained in his health records and he certainly will not know what information will be added in the future.[125] At the time of consent, he will also not be aware of the specific uses or disclosures of his health data because the form he executes may generally authorize disclosures for "treatment, payment, or health care operations." For these reasons, the person's execution of a written consent prior to treatment is uninformed. The consent also is not completely voluntary. The regulations explicitly permit providers to condition enrollment in a plan or medical treatment (in non-emergency cases) on whether the individual signs the consent document.[126] In effect, the patient is forced to consent if he wants to obtain treatment or health insurance.[127] The only practical result of an informed consent requirement is to alert the patient to the general ways in which his health data will be used and disclosed. Absent the ability to further control these uses and disclosures, this merely constitutes notice of data sharing practices.

Society benefits from a more cost-efficient health care system through faster and less expensive transactions and potential improvements in clinical care. Imposing a national informed consent requirement is burdensome on the health care system. While many health providers already require individual informed consent as part of many health care transactions, all covered entities will have to develop mechanisms to obtain, access, and store consent forms from every individual. Health care providers may also have to delay treatment to the detriment of patients if consent forms are lost or unsigned.[128]

We have argued that where the benefit to the individual is small and the burden on public services is large, privacy rules should yield. In this case, "informed consent" provides very little benefit to the individual because she has little choice but to acquiesce to the data use. At the same time, the burdens on the health care system are substantial because informed consent entails significant administrative costs in obtaining and storing consent documents. In such circumstances, the regulations neither protect privacy nor facilitate quality health care.

125. *See* Gostin, *supra* note 91, at 3017.
126. 45 C.F.R. § 164.506(b)(1), (2) (2001).
127. *See* PRITTS ET AL., *supra* note 29, at 16.
128. *See id.*

We would, therefore, eliminate the informed consent rule and replace it with an enhanced notification requirement. The electronic, free-flowing exchange of data among health care professionals, institutions, and insurers for the purposes of processing a health claim or delivering medical service implicates few individual privacy concerns, but promotes efficiency in data processing.

B. INDIVIDUAL AUTHORIZATION FOR NON-HEALTH RELATED PURPOSES

The regulations employ a different consent model for disclosures and uses of PHI unrelated to health care (e.g., for employment decisions or evaluation of credit status). The regulations incorporate an "anti-disclosure rule." Prior to use or disclosure of PHI for non-health care purposes, covered entities must obtain an authorization from the individual. Unlike the informed consent requirement for health care-related disclosures, an individual's choice is respected. The exercise of the right of refusal cannot be used to deny the patient treatment or health insurance.[129]

Also unlike the informed consent requirement, the authorization contains specific information to help individuals decide whether to permit disclosure or use. Such authorizations must (1) identify the information to be used or disclosed in a "specific and meaningful fashion";[130] (2) provide the names of the persons or organizations who will make and receive the use or disclosures;[131] (3) explain the purpose for each request; (4) notify the individual of his right to refuse to sign the authorization without negative consequences to treatment or health plan eligibility (except under specific circumstances);[132] (5) be written in plain language;[133] (6) include an expiration date;[134] and (7)

129. 45 C.F.R. § 164.508(b)(4) (2001). There are some limited exceptions. First, health care providers may condition provision of research-related treatment on authorization. *Id.* § 164.508(b)(4)(i). Second, if the covered entity is gathering individually identifiable health information solely for the purposes of disclosing it to a third party, such as an employer, the covered entity may condition this care on the authorization to disclose it to the third party. *Id.* § 164.508(b)(4)(iv). Further protection is offered regarding psychotherapy notes; authorization is always required for use and disclosure of psychotherapy notes except in specified health care operations. *Id.* § 164.508(b)(4)(ii)(B).

130. *Id.* § 164.508(c)(1)(i).

131. *Id.* § 164.508(c)(1)(ii), (iii).

132. *Id.* § 164.508(e)(1).

133. *Id.* § 164.508(c)(2).

explain that the individual has a right to revoke the authorization[135] at any time in writing except where the covered entity has already relied on the authorization.[136]

Advance written authorization for uses or disclosures of health data for non-health care purposes is an important privacy safeguard. Outside disclosures are unlike those that occur in the health care setting where information is needed to complete a health-related transaction and the risks of harm to individuals are negligible. Disclosures to public or private sector entities or persons outside the health care context can lead to significant harms. Disclosures to existing or potential employers, insurers (other than an existing health insurance company that presently needs to process a claim), governmental agencies, commercial marketers, family members, friends, neighbors, or others can negatively affect an individual's job status or opportunities, insurability, and social status. People are rightfully concerned about these types of disclosures. Under our balancing approach, individuals should have some right to control disclosures that can result in discrimination, stigmatization, or embarrassment. At the same time, outside disclosures are unlikely to achieve an important health-related objective. Providing patients with the right to control such uses of data will not undermine an important public interest.

IV. MAKING EXCEPTIONS: BALANCING COMMON GOODS AND PERSONAL PRIVACY

Through its health information privacy regulations, DHHS attempts to protect individual privacy while recognizing legitimate needs for such data to process health claims and deliver medical care, as well as provide for common goods. As we discuss above, the regulations adopt an "anti-disclosure" rule for data that are not related to health care. Thus, uses and disclosures of health data outside the health care setting are prohibited without specific, written authorization.

The regulations, however, do permit disclosures for a variety of non-health care purposes without written authorization, such as national defense and security, identification of deceased persons, and the administration of justice.[137] One of the

134. *Id.* § 164.508(c)(1)(iv).
135. *Id.* § 164.508(c)(1)(v).
136. *Id.* § 164.508(b)(5).
137. A covered entity may disclose PHI in a judicial or administrative pro-

most controversial exceptions to the "authorization" rule involves parental access to a minor's medical records. Disclosures to parents of unemancipated minors are exempted from authorization requirements depending on state law. If state law forbids or requires that parents be informed about their children's health conditions, the regulations allow state law to stand.[138] Absent any applicable state law, parents may serve as personal representatives,[139] who act on behalf of the individual[140] with some restrictions.[141]

We apply our balancing approach to five additional broad exceptions to the anti-disclosure rule: public health, health research, law enforcement, familial notification, and commercial marketing. In each context, the most important consideration is whether the loss of privacy is justified by the achievement of a substantial public purpose.

A. PUBLIC HEALTH

DHHS's privacy regulations broadly exempt[142] disclosures of PHI for routine public health activities.[143] This includes disclosures (a) where federal or state law authorizes public health authorities[144] to collect PHI to prevent or control disease, injury, or disability, or report child abuse or neglect; (b) to notify persons who may be at risk for or exposed to a communicable disease (e.g., partner notification provisions);[145] and (c) concerning adverse events, tracks, and product recalls, and post-marketing surveillance by persons subject to the jurisdiction of the Food and Drug Administration.[146] In addition, state reporting or other public health laws are not preempted by the rule

---

ceeding in response to an order of the court or administrative tribunal or, in certain circumstances, a subpoena or discovery request.

138. *See* 45 C.F.R. § 160.202 (2001) (defining a "more stringent" state law).

139. *Id.* § 164.502(g)(3).

140. *Id.* § 164.502(g)(2).

141. If the minor consents to the health care service, the parent agrees to confidentiality between provider and the minor, or the minor consents and does not wish the parent to be personal representative, then the parent is not considered a personal representative. *Id.* § 164.502(g)(3).

142. *Id.* § 164.514(b)(2) (clarifying that all of the exceptions apply to uses of PHI as well as disclosures in the public health exemptions section).

143. *See* Gostin, *supra* note 91, at 3019.

144. Public health authority is expansively defined as a federal, tribal, state, or local agency, or a person or entity with a grant of authority or contract with the agency. 45 C.F.R. § 164.501 (2001).

145. *Id.* § 164.512(b)(1)(i), (ii), (iv).

146. *Id.* § 164.512(b)(1)(iii).

even if they offer fewer privacy protections.[147] This preemptive measure leaves intact (1) existing state law requirements for the use or disclosure of identifiable health data by public health authorities; and (2) public health information privacy regulations under an inconsistent array of state laws. Even though state and local public health authorities have an excellent record of maintaining the confidentiality of identifiable health data, we (and others) have suggested the need for better privacy protections for state public health data.[148]

Despite the need for improved privacy protections for public health data at the state level, DHHS's public health exception from individual consent and authorization requirements reflects a proper balance of individual and collective interests. The benefits of public health relate to society as well as individuals. Public health practice has traditionally relied on these disclosures as authorized through federal, state, and local laws and respected the sensitive nature of the information. Though the autonomous interests of individual are infringed to some extent, the utilitarian premise that individuals should contribute to these greater goods in society sustains these types of disclosures.

B. HEALTH RESEARCH

A covered entity can use or disclose PHI for health research without individual authorization if it obtains a waiver from an Institutional Review Board (IRB) or a privacy board. To understand the significance of this provision, it will be helpful to explain current law regulating human subject research.

Most federally funded human subject research is subject to federal regulations known as the Common Rule.[149] The Common Rule does not set forth detailed privacy standards. Rather, it conditions IRB approval of government-sponsored research on whether "there are adequate provisions to protect the privacy of subjects."[150] Though the Common Rule is a helpful guide for protecting the privacy and other ethical interests of human research subjects, it does not apply to privately funded

147. *Id.* § 160.203(c) (2001).

148. Lawrence O. Gostin et al., *Informational Privacy and the Public's Health: The Model State Public Health Privacy Act*, 91 AM. J. PUB. HEALTH 1388 *passim* (2001).

149. Federal Policy for the Protection of Human Subjects, 45 C.F.R. § 46 (2001).

150. *Id.* § 46.111(a)(7).

research.

DHHS's health information privacy regulations apply more detailed privacy requirements than exist under the Common Rule. In general, specific authorization for the use or disclosure of health data for research is needed. A covered entity may, however, use or disclose PHI for research without the person's authorization if it obtains a waiver from an IRB or privacy board[151] that finds (1) the use or disclosure involves no more than minimal risk; (2) the waiver will not adversely affect the privacy rights and welfare of the individuals; (3) the research could not practicably be conducted without the waiver; (4) the privacy risks are reasonable in relation to the anticipated benefits, if any, to individuals and the importance of the research; (5) a plan exists to protect the identifiable information from improper use and disclosure; (6) a plan to destroy the identifiers exists unless there is a health or research justification for retaining them; and (7) there are written assurances that the data will not be reused or disclosed to others, except for research that would also qualify for a waiver.[152] Researchers must also show that PHI is necessary for the research, will not be disclosed to outsiders, and is sought solely for research purposes.[153]

Critics are concerned about the burdens imposed by the new requirements.[154] The regulations limit the ways that researchers can access, use, and disclose health data for research purposes. Researchers are worried that new regulations will slow or halt existing and future research efforts.[155] Yet, the regulations support the need to utilize PHI without consent, and provide a workable framework for protecting individual

151. *Id.* § 164.512(i)(1)(i). The privacy board must have members with varying backgrounds, appropriate professional competency, and no conflict of interest. *Id.* § 164.512(i)(1)(i)(B). At least one member must be unaffiliated with the covered entity and research entity. *Id.* § 164.512(i)(1)(i)(B)(2). This includes relatives of individuals affiliated with the organizations. *Id.* A majority of the privacy board must be present when considering a waiver, including the unaffiliated member. *Id.* § 164.512(i)(2)(iv)(B).

152. *Id.* § 164.512(i)(2)(ii).

153. *Id.* § 164.512(i)(1)(ii); *see* Mark Barnes & Sara Krauss, *The Effect of HIPAA on Human Subjects Research*, 10 HEALTH L. REP. 1026, 1030-31 (2001).

154. Jocelyn Kaiser, *Researchers Say Rules Are Too Restrictive*, 294 SCI. 2070 (2001); Kulynych & Korn, *supra* note 33, at 201; *see, e.g.*, Barnes & Krauss, *supra* note 153, at 1031 (suggesting that IRBs are ill-prepared to make the assessments now required of them by the health data privacy rule).

155. Kulynych & Korn, *supra* note 33, at 201.

privacy while also facilitating research. Like the use or disclosure of health data for public health, there are societal benefits to facilitating high quality clinical or health services research. Provided that the measures imposed by the regulations do not significantly thwart health research, they fit well within our balancing approach.

C. LAW ENFORCEMENT

A covered entity may disclose PHI to a law enforcement official without authorization or informed consent pursuant to a court order, subpoena, or administrative request, including a civil investigative demand or an administrative subpoena.[156] In addition, a covered entity may disclose limited information[157] without prior judicial approval where (1) the information relates to a crime victim who is incapacitated and disclosure is necessary and in the best interests of the victim;[158] (2) PHI is evidence of criminal conduct that occurred on the premises of the covered entity;[159] or (3) in the course of an emergency, disclosure is necessary to alert law enforcement to the location, commission, and nature of the crime, victims, or perpetrators.[160]

It is difficult to balance individual and collective interests in sharing health data for law enforcement purposes.[161] Indi-

156. 45 C.F.R. § 164.512(f)(1) (2001). When an administrative request is utilized, the rule lays out certain requirements: "(1) [t]he information sought is relevant and material to a legitimate law enforcement inquiry; (2) [t]he request is specific and limited in scope to the extent reasonably practicable . . . ; and (3) [d]e-identified information could not reasonably be used." *Id.* § 164.512(f)(1)(C).

157. The permitted information is name, address, date and place of birth, social security number, blood type, type of injury, date and time of treatment, and a description of distinguishing characteristics. *Id.* § 164.512(f)(2)(i).

158. *Id.* § 164.512(f)(3). The specific criteria are (1) the law enforcement official states that the information is needed to determine whether a crime occurred by an individual other than the victim and that the information will not be used against the victim; (2) the law enforcement official represents that immediate law enforcement activities would be jeopardized by waiting for consent; and (3) the covered entity determines that the disclosure is in the best interest of the individual. *Id.* § 164.512(f)(3)(iii). If the patient is competent and no emergency exists, the patient must agree under the exception for the disclosure to occur. *See id.* § 164.512(f)(3).

159. *Id.* § 164.512(f)(5).

160. *Id.* § 164.512(f)(6).

161. Peter H.W. Van Der Goes, Jr., Comment, *Opportunity Lost: Why and How to Improve the HHS-Proposed Legislation Governing Law Enforcement Access to Medical Records*, 147 U. PA. L. REV. 1009 (1999).

viduals rightfully may be concerned about the nonconsensual sharing of their data with government officials who are empowered to use these data in ways that may counter individual interests. Law enforcement, however, may have a strong claim to the data to protect the health or lives of the individual, other persons, or the community as a whole. For example, law enforcement may need to gain access to an individual's health profile to help identify a suspected bioterrorist. In these cases, law enforcement officials may oppose the federal requirement that they must first obtain a warrant, subpoena, or other court order prior to accessing individual health data.[162]

Broad disclosures to law enforcement officials can weaken the public's trust in how their health care data are used and disclosed. DHHS's privacy regulations arguably make it too easy for unauthorized disclosures to police to take place. Notably, limited disclosures may occur without a judge's approval through administrative requests. Even if a court does make the decision, the regulations do not provide clear criteria.

A better privacy rule would be to require a court order prior to disclosure, except in cases of emergencies that endanger public health and safety. Courts, moreover, need clear criteria for making decisions to allow disclosure. Judges could order disclosures, for example, if there were probable cause that the evidence was necessary for the prosecution of a serious offense or if it were necessary to prevent a serious future harm. If there were an impartial judicial process based on restrictive standards of disclosure, privacy would be protected without unduly interfering with the legitimate pursuit of crime investigation and prosecution.

D. FAMILIAL NOTIFICATION

Disclosures to family or "significant others" (i.e., friends, caretakers, or health care surrogates) of adults and emancipated minors are narrowly exempted. Covered entities may disclose limited health information to family members or "significant others" without consent if the patient is informed in advance and has the opportunity to agree.[163] The disclosed PHI

162. Sharon J. Hussong, *Medical Records and Your Privacy: Developing Federal Legislation to Protect Patient Privacy Rights*, 26 AM. J.L. & MED. 453, 458-59 (2000).

163. 45 C.F.R. § 164.510(b)(1), (2) (2001). Disclosure is also permitted if the covered entity can reasonably infer from the circumstances that the patient does not object to disclosure. *Id.* § 164.510(b)(2)(iii).

must be (1) "directly relevant to such person's involvement" with the patient's care or payment for care;[164] or (2) used to notify that person of the patient's location, general health condition, or death.[165] In cases of incapacitation or emergency, disclosures may be made in the patient's best interest when directly relevant to the entities' involvement with the individual's care.[166]

Despite health providers' concerns about interference with standard practices of notifying next of kin or others of an individual's admission, treatment, or prognosis, the regulations allow these practices to continue without extinguishing an individual's right to control the recipients and circumstances of these disclosures. An individual is entitled to expect a higher degree of autonomy surrounding these disclosures, and the regulations attempt to preserve some control without eliminating disclosures under specific circumstances.

E. COMMERCIAL MARKETING

In contrast to the other anti-disclosure exceptions, which offer either greater or similar protections than national or state laws currently provide, the exception for commercial marketing provides for less privacy protection by condoning the use or disclosure of PHI for commercial marketing without consent.[167] PHI may be used or disclosed by covered entities without individual authorization for marketing communications to the individual that (1) occur in "face-to-face encounters" (whether health-related or not[168]), (2) "[c]oncern[] products or services of nominal value," or (3) "[c]oncern[] the health-related products and services of the covered entity or of a third party."[169] Commercial communications must identify the covered entity, disclose whether the entity is receiving remuneration for the communication or sale, and instruct individuals how they can

164. *Id.* § 164.510(b)(1)(i).

165. *Id.* § 164.510(b)(1)(ii).

166. *Id.* § 164.510(b)(3). The regulations allow relatives and close personal friends to perform common care-taking duties such as picking up prescriptions and medical supplies. *Id.*

167. ROBERT GELLMAN, ANALYSIS OF THE MARKETING PROVISIONS OF THE HIPAA PRIVACY RULES (Jan. 2001), *available at* http://www.hipaadvisory.com/action/privacy/marketing.htm.

168. *Id.*

169. 45 C.F.R. § 164.514(e)(2) (2001).

opt out of receiving future communications.[170] If a covered entity targets persons based on their health status, it must predetermine whether the product or service may be beneficial to the persons and indicate why the persons have been selected.[171]

In the preamble to the regulations, DHHS explains that the covered entity need not conduct the marketing itself. It can hire out work, such as telemarketing or direct mailings, to a business associate. Furthermore, the covered entity can market products or services of a third party. Thus, the marketed goods need not be exclusively those of the covered entity.[172]

The commercial marketing exception is challengeable on many grounds: (1) It facilitates the ability of providers, insurers, pharmacists, laboratories, or their business associates to approach health consumers for a variety of commercial products or services; (2) it does not specify the basis for (or who gets to decide) what products or services are "beneficial" to patients or insureds; (3) it makes individuals unwitting participants in commercial marketing efforts[173] by requiring individuals to opt out of the communication or other marketing technique, instead of allowing them to opt in;[174] and (4) it does not require covered entities to make it easy for health consumers to opt out through toll-free numbers, postage-free mailings, or interactive websites.

Perhaps most importantly, the commercial marketing exception infringes individual privacy interests by disclosing PHI to others for non-health related purposes that most do not view as societally beneficial. Like public health authorities and health researchers, covered entities may claim a need for PHI to market products, services, or knowledge that can improve individual and communal health. However, where access to PHI is motivated by profit-oriented goals (as contrasted with

170. *Id.* § 164.514(e)(3)(i).

171. *Id.* § 164.514(e)(3)(ii).

172. Standards for the Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,461 (Dec. 28, 2000).

173. *See* Weld v. Glaxo Wellcome, Inc., 746 N.E.2d 522 (Mass. 2001) (certifying a group of individuals as a class for the purposes of challenging a pharmacy practice of using their identifiable data for a drug information program without consent).

174. DHHS has recently proposed that covered entities must obtain individual informed consent prior to sending patients marketing materials. Press Release, U.S. Dep't of Health and Human Servs., HHS Proposes Changes that Protect Privacy, Access to Care (Mar. 21, 2002), *available at* http://www.hhs.gov/news/press/2002pres/20020321a.html.

the community-oriented goals of public health or academic or non-profit research), the claim for non-consensual access to PHI is unjustified under our balancing approach. People may choose to participate in private sector marketing campaigns but should not have to. The commercial marketing exception permits potentially broad disclosures based on profit motives without individuals having an advance opportunity to object.

CONCLUSION

In the computer age where individual health data are increasingly acquired, used, disclosed, and stored in electronic formats, threats to privacy concern American consumers. The existing inadequacy of health information privacy protections and the potential for discrimination, stigmatization, or embarrassment of individuals based on misuses or wrongful disclosures of their sensitive health data justify new privacy protections. DHHS's health information privacy regulations provide a federal floor of protections that empower individuals with affirmative new rights to access and control the uses and disclosures of their health data.

Protecting individual privacy is an important objective underlying a national privacy policy, but it is not the sole aim. There are legitimate needs for sharing health data to accomplish public benefits. Achieving a balance between personal privacy and public goods is difficult. There are few guides to balancing in the extant scholarship. We suggest that to properly balance these interests, health information privacy policies should abandon a focus on individual autonomy. A national health information privacy standard should attempt to maximize individual privacy interests where the risks of harm are greatest (e.g., concerning disclosures to employers, insurers, social contacts, and commercial entities), and maximize common goods where the public interests are strongest (e.g., public health and research). Striking this balance may diminish individual autonomy in non-harmful ways, but also promises significant communal benefits.

DHHS's attempt to balance individual and communal interests in the sharing of health data through its health information privacy regulations is consistent with this approach in notable ways. For example, the requirement for written authorization for many disclosures of health data outside the health care context fulfills individual privacy interests where they matter most. Exceptions to this general requirement for

disclosures for public health and health research are warranted to further important societal objectives. However, the regulations also fail to adhere to our approach. Requiring individual informed consent for disclosures of health data for health-care related purposes is neither informed nor consensual, and does little to protect individual privacy while significantly burdening the health care system. As well, disclosure for law enforcement purposes is currently too easy, without judicial supervision based on clear standards. Finally, disclosure exceptions for commercial marketing fail to promote an important public purpose and can lead to breaches of privacy. Thus, while new health information privacy regulations are a key step forward in the pursuit of a cohesive national health data policy, additional progress on balancing the sharing of health data for communal purposes and protecting individual privacy interests is needed.