2010

Protecting Privacy in Health Research: The Limits of Individual Choice

Fred H. Cate
Indiana University Maurer School of Law, fcate@indiana.edu

1-1-2010

Protecting Privacy in Health Research: The Limits of Individual Choice

Fred H. Cate
Indiana University Maurer School of Law, fcate@indiana.edu

Protecting Privacy in Health Research: The Limits of Individual Choice

Fred H. Cate†

† Fred H. Cate is a Distinguished Professor, C. Ben Dutton Professor of Law, director of the Center for Applied Cybersecurity Research, and director of the Center for Law, Ethics, and Applied Research in Health Information at Indiana University, and a senior policy advisor to the Centre for Information Policy Leadership at Hunton & Williams LLP. The author is grateful for the insights and support of Beth Cate, Stan Crosley, Aviva Orenstein, Paul Schwartz, and his colleagues in the Protecting Privacy in Health Research Project; the excellent research assistance of Kathryn Pardo; and the patience of the editors of the *California Law Review*. This Article is based in part on research funded by the National Institutes of Health (RC1 CA146501-01) and the Lilly Endowment Inc.

INTRODUCTION

In his groundbreaking 1967 study, *Privacy and Freedom*, Alan Westin defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[1] Many data protection laws enacted since then have followed suit, relying on choice—often together with notice necessary to support choice—as the key tool for protecting privacy, or even as the *goal* of those laws.

For example, the influential *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, adopted by the Committee of Ministers of the Organization for Economic Cooperation and Development (OECD) in 1980, provide that personal data should not be used for purposes other than those specified at the time the data were collected, except: "(a) with the consent of the data subject; or (b) by the authority of law."[2]

Additionally, the Data Protection Directive adopted by the European Union (EU) in 1995 is significantly focused on individual choice. According to the directive, data protection is achieved in part through "the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances."[3] Article 7 of the directive provides seven conditions under which personal data may be processed. The first is when "the data subject has unambiguously given his consent."[4] Article 8 restricts the processing of sensitive data, but then provides that the restriction shall not apply where "the data subject has given his explicit consent to the

1. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

2. ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 15 (1980), *available at* http://www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html.

3. Council Directive 95/46, Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Preamble ¶ 25, 1995 O.J. (L281) (EC), *available at* http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Directive&an_doc=1995&nu_doc=46.

4. *Id*. art. 7(a).

processing of those data."[5] Finally, Article 26 identifies six exceptions to the provision prohibiting the export of personal data to non-European countries lacking "adequate" data protection. The first is that "the data subject has given his consent unambiguously to the proposed transfer."[6]

The Asia-Pacific Economic Cooperation (APEC) Privacy Framework, adopted in 2004, is similarly focused on choice: "Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information."[7]

Professor Paul Schwartz has described the focus on individual choice reflected in these laws as "privacy-control": "From the age of computer mainframes in the 1960s to the current reign of the Internet's decentralized networks, academics and the law have gravitated towards the idea of privacy as a personal right to control the use of one's data."[8] As a result, Schwartz concludes, "[t]he conventional wisdom seeks to place the individual at the center of decisionmaking about personal information use by conceiving of privacy as a right of control over data use."[9] Many privacy scholars agree, whether writing in the 1960s[10] or the current millennium.[11]

Nowhere is the focus on individual choice, and notice to facilitate that choice, more evident than in the United States. Beginning in the mid-1990s, the Federal Trade Commission (FTC) and state attorneys general encouraged U.S. operators of commercial websites to adopt and publish online privacy policies. Adoption of such policies was voluntary; compliance with them was not. The Commission interprets section 5 of the Federal Trade Commission Act, which empowers the FTC to prosecute "unfair and deceptive" trade practices, to include violations of posted privacy policies.[12]

---

5. *Id.* art. 8(2)(a).

6. *Id.* art. 26(1)(a).

7. Asia-Pacific Economic Cooperation, APEC Privacy Framework, 2004/AMM/014rev1 (Nov. 2004), at 12, *available at* http://www.apec.org/apec/news___media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/ministerial/annual/2004.Par.0015.File.v1.1.

8. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1659 (1999).

9. *Id.* at 1660.

10. Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) (describing privacy as "the *control* we have over information about ourselves").

11. A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1463 (2000) (describing privacy as "the ability to control the acquisition or release of information about oneself"); HELEN NISSENBAUM, PRIVACY IN CONTEXT 70 (2010) (criticizing "conceptions of privacy adopted in scholarship, law, and policy [that] incorporate control as a component of privacy, or, one might say, constitute privacy as a particular form of control").

12. 15 U.S.C. § 45(a)(1) (2006); FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 8–9 (2010) [hereinafter PROTECTING CONSUMER PRIVACY], *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

In 1998, the FTC reported to Congress on what it believed a privacy policy must contain. After reviewing the "fair information practice codes" of the United States, Canada, and Europe, the Commission concluded: "Common to all of these documents . . . are five core principles of privacy protection," the first two of which were "Notice/Awareness" and "Choice/Consent."[13] According to the Commission, "[t]he most fundamental principle is notice. . . . [because] [w]ithout notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information."[14] The FTC continued, "[t]he second widely-accepted core principle of fair information practice is consumer choice or consent . . . [over] how any personal information collected from them may be used."[15]

U.S. statutes and regulations have tended to parallel the FTC's choice-based approach. For example, in 1999 Congress passed major financial privacy legislation as Title V of the Gramm-Leach-Bliley Financial Services Modernization Act.[16] The law permits a financial institution to transfer any "nonpublic personal information" to nonaffiliated third parties only if the institution "clearly and conspicuously" provides consumers with a notice about its information disclosure policies and an opportunity to opt out of such transfers.[17] That notice must be sent at least annually even if there is no change in its terms. [18]

The Privacy Rule applicable to personal health information, adopted in 2001 by the U.S. Department of Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act (HIPAA), provides a starker example.[19] First, the rule permits a covered entity to use personal health information to provide, or obtain payment for, health care only after first providing the patient with notice and making a good faith effort to obtain an "acknowledgment."[20] Second, for most purposes other than treatment or payment, a covered entity may use personal health information only with an individual's opt-in "authorization."[21] Third, a covered entity may use or disclose personal health information for directories and to notify and involve other individuals in the care of a patient if the covered entity obtains the

13. FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf.

14. *Id*. at 7.

15. *Id*. at 8 (citations omitted).

16. Gramm-Leach-Bliley Financial Services Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

17. *Id*. §§ 502(b)(1), 503(b)(1)(B).

18. *See id*. § 503(a).

19. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,461 (Dec. 28, 2000) (as amended by 67 Fed. Reg. 53,181 (Aug. 14, 2002) (codified at 45 C.F.R. pt. 160, §§ 164.502, 164.506)).

20. 45 C.F.R. § 164.506(a) (2009).

21. *Id*. § 164.508(a)(1).

"agreement" of the individual.[22] Thus, the health Privacy Rule well illustrates the centrality and growing complexity of notice and consent requirements: one rule to deal with one type of information requires the use of three different types of notice and consent.

In fact, the focus on choice has done more to undermine—rather than to protect—individual privacy, and to diminish—rather than to maximize—human welfare. The reasons this is true may be divided into two broad categories. The first includes objections relating to how choice works in practice. All of the available evidence suggests that notices are widely ignored by individuals and are written in overly broad or overly detailed language.[23] As a result, individuals are not aware of—or do not understand—the choices available to them, or those choices are so broad or so frequent as to be meaningless.

The second category includes objections to the concept of defining privacy as individual control and hinging its protection on decisions by individuals. Individual choice is not the same as personal privacy, so focusing laws, regulations, and enforcement on the former will not necessarily enhance the latter. As the Institute of Medicine (IOM) Committee on Health Research and the Privacy of Health Information wrote in 2009, "consent (authorization) itself cannot achieve the separate aim of privacy protection."[24] Moreover, the preoccupation with choice effectively shifts the burden for protecting privacy from the data user to the data subject. Choice can be a disservice to the individual, for example, when the individual injures his or her own interests through an uninformed or unwise choice. And there are many situations in which individual choice is outweighed by other interests of the individual or society. For example, we do not ask licensed professionals (such as airplane pilots or childcare workers) to agree to have their personal information collected and processed, yet this does not mean that they have no privacy interests in the subsequent reuse or disclosure of that information.

In short, the control-based system of data protection is not working. The flurry of notices may give individuals some illusion of enhanced privacy, but the reality is far different. The result is the worst of all worlds: privacy protection is not enhanced, individuals pay the cost of bureaucratic laws, and we have become so enamored with notice and choice that we have failed to develop better alternatives. The situation only grows worse as new technologies and applications increase the supply of, and the demand for, personal information.

22. *Id.* § 164.510.

23. PROTECTING CONSUMER PRIVACY, *supra* note 12, at iii, 19–20.

24. BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 250 (Sharyl J. Nass et al. eds., 2009), *available at* http://books.nap.edu/openbook.php?record_id=12458.

In the specific context of using personal information for health research, both sets of objections—those relating to practical implementation and those relating to the fundamental concept of choice-based systems—are present.[25] As a practical matter, it is very difficult to make a meaningful choice-based system work, and there are strong ethical objections to making life-saving health research depend on individual choice to use information.

Rather than examine the limits of choice broadly as the dominant means of protecting privacy, as has been done before,[26] this Article addresses those limits in the specific context of using personal information for health research. There are five reasons this is a particularly appropriate context in which to consider the role of choice. First, it is an area in which both the value and the limits of choice are particularly evident. Second, it is an area of great importance to individuals and society more broadly. Third, it is an area where there has been considerable recent and on-going attention as part of both the national debate over health care reform and multinational discussions about data protection reform. Fourth, in part because of that recent attention, it is an area in which society might be able to speak meaningfully about solutions—that provide more ethical, and more efficient approaches to data protection than relying on individual choice. Finally, the analysis and problem-solving we bring to this area can provide useful guidance in other contexts.

Part I of this Article briefly surveys the objections to relying on consumer choice for protecting privacy generally, before examining the role of individual choice in health research in particular. Part II provides an introduction to health research and its regulation. It discusses the expanding role of personal information, the ethical principles of autonomy and informed consent, and the primary federal regulation of health research—the Common Rule. Part III examines the Privacy Rule issued under HIPAA. Part IV considers the impact of the Privacy Rule and its consent requirement on both health research and personal privacy. Finally, Part V offers some tentative thinking about ways of improving the operation of consent, as well as alternatives to consent.

This Article argues that an inappropriate reliance on individual choice concerning the use of personal information in health research has disserved both individuals and society. While many of the reasons are practical, and have to do with the difficulty and cost of obtaining any choice—whether positive or negative—there are substantial conceptual objections to relying so heavily on individual choice in this setting, including that it is unethical to do so.

---

25. "Research" is defined under both the Privacy Rule and the Common Rule as "a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge." 45 C.F.R. §§ 46.102(d), 164.501 (2009).

26. *See, e.g.*, Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 343 (Jane K. Winn ed., 2006), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972.

I.
THE CRITIQUE OF CHOICE

While focusing on choice, and mandatory notices to support individual choice, has long been a favored strategy of lawmakers, regulators, and privacy advocates, today there is mounting criticism that choice is, at minimum, insufficient and, in many cases, undesirable. A lengthy analysis of the broad critique of choice is beyond the scope of this Article, but a brief summary of those objections is useful to place the analysis of choice as applied to data protection in health research in broader context.

A. Inaccessibility

Notices are often inaccessible. Many notices in the United States are complex because the laws and business practices they describe are complex. Moreover, they often read like contracts because regulators have chosen to enforce them like contracts.[27] eBay Vice President and General Counsel Kent Walker has written that notices often suffer from:

- "Overkill"—"masses of unintelligible small print that no one bothers to read."[28]
- "Irrelevance"—describing activities of so little concern to most consumers that it "is like leading a satiated horse to unappealing water."[29]
- "Opacity"—reflecting the "bedrock truth . . . that it is difficult to track, let alone describe, all the information that is exchanged in a typical transaction, all the places that it is stored, and all the ways that it is used."[30]
- "Non-comparability"—again reflecting an underlying reality that "the simplification necessary for comparability comes at a significant cost in accuracy and flexibility."[31]
- "Inflexibility"—failing to keep pace with "new business models and new consumer demands."[32]

The opposite is often seen under European data protection laws, which can reduce notices to mere warnings. One popular privacy notice throughout London and other European capitals is "Warning: CCTV [Closed Circuit Television] in use."[33] Such signs may motivate good behavior, but they do little

27. *See, e.g.*, In the Matter of Eli Lilly and Company, FTC File No. 012 3214, Docket No. C-4047, Complaint (May 10, 2002), *available at* http://www.ftc.gov/os/2002/05/elilillycmp.htm.

28. Kent Walker, *The Costs of Privacy*, 25 HARV. J.L. & PUB. POL'Y 87, 107 (2001).

29. *Id.* at 108.

30. *Id.* at 110.

31. *Id.* at 111.

32. *Id.* at 112.

33. Department of Homeland Security, Privacy Office, Public Workshop, CCTV: Developing Privacy Best Practices, Panel on Legal and Policy Perspectives, Arlington, VA, Dec.

to empower individuals to make informed choices about the collection and use of data about them. Neither approach—loading notices with exceptional detail or reducing notices to mere cigarette-pack-like warnings—has proved very informative or protective of privacy.

B. Inadequate to Motivate Action

Few people read notices or act on consent requests unless they are required to, in which case they almost always grant consent if necessary to get the service or product they want. As FTC Chairman Jon Leibowitz noted at the first of the Commission's three 2009–2010 Roundtables on Exploring Privacy: "We all agree that consumers don't read privacy policies"[34]—a remarkable acknowledgement from the U.S. federal agency that has probably done the most to promote them.

In reality, this has long been the view of leaders of the FTC. The lack of consumer response to Gramm-Leach-Bliley financial privacy notices prompted then-FTC Chairman Timothy Muris to comment at the end of 2001:

> The recent experience with Gramm-Leach-Bliley privacy notices should give everyone pause about whether we know enough to implement effectively broad-based legislation based on notices. Acres of trees died to produce a blizzard of barely comprehensible privacy notices. Indeed, this is a statute that only lawyers could love—until they found out it applied to them.[35]

The difficulties of reaching and provoking a response from consumers are exacerbated where the party wishing to use the information has no (and may not have ever had) direct contact with the consumer. For example, most mailing lists are obtained from third parties.[36] To require the purchaser of a list to contact every person individually to obtain consent to use the names and addresses on the list would cause delay, require additional contacts with consumers, and almost certainly prove prohibitively expensive. And it could not be done without using the very information that the list purchaser is seeking consent to use.

C. The Absence of Choice

Notices often merely disclose the absence of choice. For example, the Gramm-Leach-Bliley financial privacy provisions, under which Congress

---

18, 2007 (statement of Fred H. Cate), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_workshop_cctv_Transcript_Legal_and_Policy_Perspectives_Panel.pdf.

34. Jon Leibowitz, Chairman, Fed. Trade Comm'n, Introductory Remarks at the FTC Privacy Roundtable (Dec. 7, 2009), *available at* http://www.ftc.gov/speeches/leibowitz/091207privacyremarks.pdf.

35. Timothy J. Muris, Chairman, Fed. Trade Comm'n, Remarks at the Privacy 2001 Conference (Oct. 4, 2001), *available at* http://www.ftc.gov/speeches/muris/privisp1002.shtm.

36. ROBERT O'HARROW, JR., NO PLACE TO HIDE 34–73 (2005).

requires that financial institutions send notices to customers annually even if there has been no change in the institution's privacy practices, in fact require just *one* consumer choice: consumers can opt out of some, but not all, transfers of personal information to third parties for marketing purposes.[37] As a practical matter, therefore, consumers' only serious choice in response to the notices is to choose to take their business elsewhere, assuming there is another financial institution that discloses preferable data processing practices.

D. The Illusion of Choice

Notice and choice opportunities are often so broad as to make choice meaningless. Schwartz has noted: "One's clicking through a consent screen to signify surrendering of her personal data for all future purposes is an example of both uninformed consent and a bad bargain."[38] Similarly, when choice is offered for a service or product that cannot be provided without personal information, individuals are afforded the illusion—but not the reality—of choice.

European data protection regulators have addressed this issue in the context of employers asking employees to consent to the collection and use of personal information. The Article 29 Working Party, made up of the national data protection commissioners from each of the twenty-seven EU member states, has expressed the view that where "consent is required from a worker, and there is a real or potential relevant prejudice that arises from not consenting, the consent is not valid."[39] The Working Party has made this point repeatedly: "If it is not possible for the worker to refuse it is not consent."[40] "Consent must at all times be freely given. Thus a worker must be able to withdraw consent without prejudice."[41] As a result of these views, consent is rarely a basis for data processing in employment contexts in Europe; processing must be justified on some basis other than consumer choice.

E. Inadequate Privacy Protection

Individual choice is not the same thing as privacy protection and merely providing choice does not necessarily enhance privacy protection. Choice—and notice to support choice—have tended to become a distraction from, or even a substitute for, more meaningful privacy protections. As a result, the energy of data processors, legislators, and enforcement authorities is often expended on notices and choice opportunities, rather than on enhancing privacy. Compliance

37. Gramm-Leach-Bliley Financial Services Modernization Act, Pub. L. No. 106-102, § 502(b)(2), (e), 113 Stat. 1338, 1437, 1438 (1999).

38. Schwartz, *supra* note 8, at 1678.

39. *Article 29 Working Party Opinion on the Processing of Personal Data in the Employment Context*, at 23, WP 48 (Sept. 13, 2001), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48en.pdf.

40. *Id.*

41. *Id.*

with data protection laws is often focused on providing required notices in proper form at the right time and acting on choices, rather than on ensuring that personal information is protected.

Data breach notification laws are an unfortunate, but timely, example. Beginning with California in 2002, forty-three states and the District of Columbia have adopted security breach legislation.[42] These laws all have in common the requirement that institutions suffering breaches of personal information must notify the individuals whose data are involved. Now the United Kingdom,[43] Canada,[44] New Zealand,[45] Australia,[46] and other countries are considering similar laws. But notices only *respond* to breaches; they do not *prevent* them. Moreover, while notices may appear to give recipients choices, in reality they do not, since there is not much that individuals can do after the breach has occurred. Yet regulators and legislators have flocked to breach notice laws, thus diverting government, industry, and public attention away from more pressing security threats—such as malicious code and increasingly sophisticated behavioral attacks—and more effective measures for preventing harm.[47]

Notice after the fact is too modest a response if we think data breaches pose serious security threats, and too burdensome a response if we think they do not. Accordingly, a privacy policy based on individual choice often provides too little protection for privacy, unless we think there is virtually no risk at all, in which case it is imposing unnecessary burdens on individuals and institutions alike.

---

42. For up-to-date information on state security breach laws, see *State Security Breach Notification Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm (last visited Oct. 14, 2010).

43. Information Commissioner's Office of the United Kingdom, Guidance on Data Security Breach Management (Mar. 27, 2008), *available at* http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/guidance_on_data_security_breach_management.pdf.

44. Office of the Privacy Commissioner of Canada, Key Steps for Organizations in Responding to Privacy Breaches (Aug. 28, 2007), *available at* http://www.privcom.gc.ca/information/guide/2007/gl_070801_02_e.asp.

45. Privacy Commissioner of New Zealand, Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist (Feb. 2008), *available at* http://privacy.org.nz/assets/Files/Privacy-Breach-Guidelines/Privacy-breach-guidelines-key-steps.February-2008.doc; Office of the Privacy Commissioner of New Zealand, Information Paper to Accompany Privacy Breach Guidance Material (Feb. 2008), *available at* www.privacy.org.nz/assets/Files/560990.doc.

46. Office of the Privacy Commissioner of the Australian Government, Consultation Paper: Draft Voluntary Information Security Breach Notification Guide (Apr. 2008), *available at* http://www.privacy.gov.au/publications/breach_0408.pdf.

47. *See* FRED H. CATE, INFORMATION SECURITY BREACHES: LOOKING BACK AND THINKING AHEAD 2 (2008), *available at* http://www.hunton.com/files/tbl_s47Details/FileUpload265/2308/Information_Security_Breaches_Cate.pdf.

F. False Dichotomy

The preoccupation with choice often sets up an artificial dichotomy between personally identifiable information and non-personally identifiable information. While businesses are forced to ask about the use of specific information defined by laws and regulations as personally identifiable, thousands of other potentially identifying data elements are ignored entirely. For example, while collecting (or disclosing) names and addresses may be conditioned on consumer choice, no such requirement applies to other data points, such as browser choice and font size, even though when enough of these are linked they provide an accurate, unique online identifier.[48] A 2009 study in the *Proceedings of the National Academy of Sciences* demonstrates that Social Security Numbers can actually be predicted from publicly available information about many citizens.[49] Efforts to distinguish between personally identifiable and non-personally identifiable information ignore the reality that the highly interconnected nature of the Internet, and the vast and growing volume of data found there, make even the most innocuous-seeming information capable of being linked to an identified individual.

G. Burden on the Individual

Linking privacy to individual choice can impose significant burdens on individuals, particularly as the volume and pace of data flows increase. Choice-based data protection systems have the effect of shifting the burden for protecting privacy from the data user to the data subject, yet few individuals have the time, knowledge, or interest to make all of those choices about data collection and use. To take just one example, consumer credit reports in the United States are updated with an average of 4.5 billion pieces of data per month.[50] How many people want to be asked to consent each time? Yet how meaningful is consent if it must be given or withheld for all updates as a group?

We know how consistently individuals ignore notices—not just related to privacy, but including copyright notices when downloading software, disclosure terms when opening financial accounts, and informed consent notices for medical treatments.[51] As a result, individuals may be making significant choices when they are not aware that they are making any at all. Or

48. *See* Jeremy Kirk, *EFF: Browsers Can Leave a Unique Trail on the Web*, PC WORLD, Jan. 29, 2010, *available at* http://www.pcworld.com/article/188134/eff_browsers_can_leave_a_unique_trail_on_the_web.html. For a practical demonstration visit PANOPTICLICK, https://panopticlick.eff.org/ (last visited Oct. 14, 2010).

49. Alessandro Acquisti & Ralph Gross, *Predicting Social Security Numbers from Public Data*, 106 PROC. NAT'L ACAD. SCI. 10975 (2009).

50. *FAQs, How Accurate Is the Information in a Credit Report?*, CONSUMER DATA INDUSTRY ASSOCIATION, http://www.cdiaonline.org/ConsumerInfo/content.cfm?ItemNumber=875 (last visited Oct. 14, 2010).

51. Fred H. Cate, "*The Failure of Fair Information Practice Principles*," *in* JANE K. WINN, ED., CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 341, 358–360 (2006).

they may make the choices they are forced into in order to obtain products and services they want. For example, how many consumers have ever read an intellectual property pop-up notice when attempting to download data or software? Yet in a choice-based system, those decisions can have serious consequences, such as assuming liability or waiving legal protections, even though we know they were made reflexively, without thought, or maybe not at all. Notice and choice do not protect us from our own bad, ignorant, unintentional, or unavoidable choices. Contrast choice in privacy with other types of consumer protection laws: under U.S. law, a consumer cannot consent to be defrauded, but she can consent to have her privacy violated.[52]

H. The Cost of Providing Choice

The cost of providing choice can be considerable. It can include the financial cost of creating, printing, and mailing billions of notices each year, as well as the mechanisms for recording consumer choices. This cost also includes the consequences of obtaining and acting on choice.[53] For example, under the EU Data Protection Directive, a business may transfer personal data out of the EU to a country, such as the United States, that lacks "adequate" data protection only under five conditions.[54] One of those conditions is "unambiguous consent" by the data subject.[55] What does a business relying on consent do if one customer objects: Build a separate data center in Europe? Refuse to do business with that customer? Choices have real consequences that impose real costs on individuals and institutions.

I. Government Access to Personal Data Unaffected

Notice and choice do not restrict government access to personal information, which may very well be the greatest and fastest-growing threat to personal liberty today. For instance, the government does not seek consent before requiring individuals to file taxes, obtain licenses, or register for government benefits.[56] It does not check with data subjects before intercepting

52. *See* Cate, *supra* note 26, at 374.

53. *See id*. at 364.

54. Council Directive 95/46, *supra* note 3, art. 25–26.

55. *Id*. art. 26(1)(a). The European Data Protection Supervisor describes the following requirements for "unambiguous consent": "Before a data subject can be considered to **freely** have given consent to a specific processing operation, he or she must receive **sufficient information** to be able to understand the scope and consequences of consent, including the advantages and/or disadvantages of the processing." *Legitimate Reasons for Processing of Personal Data*, EUROPEAN DATA PROTECTION SUPERVISOR, http://www.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA/QA6 (last visited Oct. 14, 2010).

56. *See* Lillian R. BeVier, *Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection*, 4 WM. & MARY BILL RTS. J. 455, 456 (1995) ("[C]itizens cannot pay taxes without at the same time providing the government with quite detailed information about their families, jobs, investments, misfortunes, and favorite charities.").

telephone calls, email messages, and other communications.[57] As the government has expanded its collection of personal data from the private sector, it does not pause to ask for individual permission before requiring employers, financial institutions, airlines, telephone companies, and thousands of other businesses to disclose billions of customer records to the government each year.[58] Moreover, the government does not care what choices the regulated businesses have offered their customers.[59] It is no defense, when the government comes calling, to say "We promised our customers and employees that we would respect their privacy by not giving the government their personal data." So, in fact, many of the so-called "privacy choices" that individuals are asked to make are misleading, because while they may purport to offer individuals some right in nondisclosure, government demands trump that right.

J. Choice As a Disservice to Individuals

Finally, choice can actually interfere with engaging in an activity of great value to individuals or society more broadly. Consider information about individuals' creditworthiness: its value derives from the fact that the information is obtained routinely, over time, from sources other than the consumer. Allowing the consumer to block use of unfavorable information would make the credit report useless. In the words of former FTC Chairman Timothy Muris, the credit reporting system "works because, without anybody's consent, very sensitive information about a person's credit history is given to the credit reporting agencies. If consent were required, and consumers could decide—on a creditor-by-creditor basis—whether they wanted their information reported, the system would collapse."[60]

In sum, individual choice as a basis for the use of personal data presents many challenges. Some of those concern the difficulties of making choice work: the inaccessibility of consent opportunities and notices, their inadequacy to provoke individuals to take action, the limited opportunities they often provide, and the considerable costs that choice can impose. But many of the challenges reflect fundamental objections to reliance on individual choice at all. These include when the choice is illusory, when choice substitutes for more meaningful privacy protection, when choice creates a false dichotomy between personally identifiable and non-personally identifiable information, when choice imposes an impossible burden on individuals, when choice leaves sensitive personal information exposed to government surveillance, and when

57. *See* Amended Complaint for Damages, Declaratory and Injunctive Relief at ¶ 6, Hepting v. AT&T Corp., No. C-06-0672-JCS (N.D. Cal. Feb. 22, 2006), *available at* http://www.eff.org/legal/cases/att/att_complaint_amended.pdf.

58. *See* Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435 (2008).

59. *See id.*

60. Muris, *supra* note 35.

choice actively disserves the best interests of individuals. These same objections are true of choices concerning the use of health data in medical research, the context on which the remainder of this Article is focused.

II.
HEALTH RESEARCH AND ITS REGULATION

A. The Role of Personal Data in Health Research

Healthcare today is increasingly information driven. It was this realization that was much of the impetus behind the passage of HIPAA—to provide for the digitization and standardization of health records necessary to enhance efficiency, accountability, and transferability of those records.[61]

However, in the fourteen years since HIPAA was passed, personal information has assumed even greater importance, especially in health research. For example, a growing volume of research no longer involves experimenting on patients and research subjects. Rather, this research focuses on reviewing data about actual experience with treatments and drug therapies in order to detect harmful side effects, to better understand the operation of medicines, to develop new treatments, and to spot unanticipated benefits and uses for drug therapies. In addition, retrospective studies—research that relies on existing data about previous medical experiences—are playing a rapidly growing role in medical research as more data about medical experiences become available in digital, structured form. Finally, major new databases have been created to facilitate research concerning cancer (e.g., the Cancer Biomedical Informatics Grid), patients requiring circulation support (e.g., the Interagency Registry for Mechanically Assisted Circulatory Support), failing organ systems (e.g., the Extracorporeal Life Support Organization), and organ transplantation (e.g., the United Network for Organ Sharing), to name just a few.[62]

1. Information-Based Health Research

The increased use of personal information in health research has been found to have many advantages. In 2009, the IOM published the report of its Committee on Health Research and the Privacy of Health Information.[63] According to that report, the advantages of information-based health research include that:

- it is often faster and less expensive than experimental studies;
- it can analyze very large sets of data;
- it may detect unexpected phenomena or differences among

61. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 261, 110 Stat. 1936, 2021.

62. BEYOND THE HIPAA PRIVACY RULE, *supra* note 24, at 116–18.

63. *See id*.

subpopulations that might not be included in a controlled experimental study;

- it can often be undertaken when controlled trials are simply not possible for ethical, technical, or other reasons;
- it can be used to study effectiveness of a specific test or intervention in clinical practice, rather than just the efficacy as determined by a controlled experimental study;
- it can also reexamine data accrued in other research studies, such as clinical trials, to answer new questions quickly and inexpensively.[64]

Reliable, accessible patient data are also critical for finding appropriate research subjects for experimental research and for developing appropriate research designs and protocols. The inability to identify and locate appropriate research subjects is a significant contributor to delaying the approval of new drugs. As the IOM committee noted: "Many research studies, especially those focused on rare conditions with limited eligible patient populations, rely on large-scale medical chart reviews and searches of patient databases to identify patients who might be eligible for and might benefit from a particular study."[65]

For example, when Eli Lilly was developing inhalable insulin, one potential concern was how the therapy would be tolerated by people with asthma or chronic obstructive pulmonary disease—the leading cause of death, illness, and disability in the United States.[66] Conducting the research necessary to answer those questions required the difficult task of locating insulin-dependent diabetics with asthma or chronic obstructive pulmonary disease who are not on inhaler therapy. In the case of chronic obstructive pulmonary disease, it also required locating diabetics who had never smoked—a near-impossibility, given that smoking is a major contributor to chronic obstructive pulmonary disease.[67] Access to patient records was critical to accomplishing this.

2. Personalized Medicine and Genetic Analysis

Information-based research is also critical to the development of personalized medicine. Personalized medicine "tailor[s] prevention strategies and treatments to each individual based on his/her genetic composition and health history."[68] For example, pharmacogenomics—the science of tailoring drug therapies to specific genetic make-ups—is a major and growing focus of

64. *Id*. at 118.

65. *Id*. at 42.

66. CTRS. FOR DISEASE CONTROL & PREVENTION, DEP'T. OF HEALTH & HUMAN SERVS., FACTS ABOUT CHRONIC OBSTRUCTIVE PULMONARY DISEASE 1 (2003), *available at* http://www.hhs.state.ne.us/menshealth/copdfaq1.pdf.

67. *Id*.

68. BEYOND THE HIPAA PRIVACY RULE, *supra* note 24, at 119.

the Food and Drug Administration (FDA), pharmaceutical companies, and medical researchers.[69] The goal is to create drugs, determine dosage and therapies, and prevent harmful and even life-threatening reactions, all based on human genotype.[70]

It sounds very futuristic, but it is happening already. In 2007, the FDA approved its first drug labeling requirement that specifically includes a warning for people with a specific genotype.[71] The drug affected by this labeling requirement is the blood thinner Coumadin (warfarin).[72] While it is a lifesaver for tens of millions of people who take it to prevent blood clots, heart attacks, and strokes, for about one-third of patients with a distinct variation of two genes, the drug can cause life-threatening internal bleeding.[73] In fact, it is the second most common drug—after insulin—implicated in visits to emergency rooms for adverse drug events.[74] The new labeling requirement warns patients and physicians about this genetic sensitivity. However, for patients to benefit from these advances, physicians must have access to individual genetic information to identify which patients are at risk.

In short, many life-saving treatments also have the potential to kill or harm. Genetic research is already helping researchers identify at-risk patients so that they can receive alternative treatments. For example, patients with two copies of the gene for an abnormal clotting factor face a 50 to 100 times greater risk of developing blood clots in the leg than the general population.[75] Physicians use this information when caring for patients who may be immobilized for a substantial period, such as following major surgery.[76]

Genetic analysis is also becoming part of standard care for treatment of many cancers. These analyses are used both to diagnose the disease and to determine responsiveness to treatment therapies. In 2006, Jonathan B. Perlin, former Undersecretary of the Department of Veterans Affairs, testified before Congress that "[c]ancer screening based on molecular genetic and proteomic tests identifies the disease earlier in many patients, giving us the opportunity to save many patients who, in fact, once could not be cured."[77]

---

69. Department of Energy, Human Genome Project Information, *Pharmacogenomics*, *available at* http://www.ornl.gov/sci/techresources/Human_Genome/medicine/pharma.shtml.

70. *Id.*

71. *FDA Updates Labeling for Blood-thinners Coumadin and Warfarin*, MEDICAL DEVICE WEEK, Aug. 20, 2007.

72. *See id.*

73. *Id*.

74. *Id*.

75. *Department of Veterans' Affairs Medical and Prosthetic Research Program: Oversight Hearing Before the H. Comm. on Veterans' Affairs*, 109th Cong. 6 (2006) (statement of Jonathan B. Perlin, Undersecretary for Health, Department of Veterans' Affairs), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_house_hearings&docid=f:28125.pdf.

76. *Id.*

77. *Id*. at 7.

The goal is to give "the appropriate drug, at the appropriate dose, to the appropriate patient, at the appropriate time."[78] However, genetic treatment therapies that focus on smaller and smaller subsets of the population make it difficult for researchers to find a large enough research population with one distinct genotype. Access to large amounts of personal data is essential to identify genetic patterns and to determine who should receive a genotype-based therapy. Access is also necessary to identify and recruit research subjects that meet ever more specific and hard-to-satisfy criteria. Thanks to remarkable advances in the study of genetics, and in information technologies necessary to collect and aggregate information about individuals' genetic markers, researchers are moving closer to achieving this goal. But doing so requires reliable access to personal information.

3. Data-Based Health Research

Data-based health research will also expand as more patient data becomes available in digital format, especially through the growth of Electronic Health Records (EHRs). EHRs are a major focus of the 2004 initiative, launched by President Bush and expanded by President Obama, to promote health information technology.[79] This initiative, overseen by the National Coordinator for Health Information Technology in the Department of Health and Human Services, seeks to lower health care costs, reduce medical errors, improve quality of care, and provide better information for patients and physicians.[80] These efforts include the distribution of $19.2 billion in grants and incentives for the development and adoption of health information technology and new requirements for the use of EHRs as a condition of receiving Medicare and Medicaid reimbursement.[81] The ultimate goal is to make virtually all patient information available electronically, which may be readily accessed by health care providers irrespective of physical location.[82]

This collection of digital records holds tremendous promise for data-based health research. As of 2009, 17 percent of U.S. physicians and approximately 8 to 10 percent of U.S. hospitals used EHRs.[83] As these figures grow, an

78. BEYOND THE HIPAA PRIVACY RULE, *supra* note 24, at 119.

79. Michael D. Rosenthal, *Electronic Health Records: A Boom or Bust for Venture Investors?*, VENTURE CAPITAL REV. 1 (Spring 2010) (noting that "the Obama and Bush administrations have put great emphasis on the development of an integrated national electronic health record (EHR) system"), *available at* http://www.snrdenton.com/news__insights/publications/idoc.ashx?docid=edaaa0dc-89be-4106-a9e9-c7bfdaf00ed9&version=-1.

80. President George W. Bush, Exec. Order No. 13335, 69 Fed. Reg. 24,059 (Apr. 27, 2004).

81. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 4102, 123 Stat. 115, 467.

82. *Id.*

83. David Blumenthal, *The Federal Role in Promoting Health Information Technology* THE COMMONWEALTH FUND, Jan. 2009, *available at* http://www.commonwealthfund.org/Content/Publications/Perspectives-on-Health-Reform-Briefs/2009/Jan/The-Federal-Role-in-

extraordinary volume of structured, digital data will potentially be available for analysis by researchers, thus expanding the range of studies that can be conducted using data on actual patient experience alone, without any testing or additional burden on patients.[84]

Moreover, valuable personal health data are increasingly generated and used outside of traditional healthcare institutions. The rise of cheap, mobile, and pervasive computing technologies that allow continuous, instant, and ubiquitous access to information is facilitating a new paradigm in which technology pushes healthcare delivery out of the clinical setting and into patients' everyday lives. PDAs, cell phones, and other "non-medical" devices are increasingly used to provide an astonishing array of health data that can provide tailored healthcare at a lower cost and empower patients and their families to manage their health more effectively.[85] These devices can be used to improve healthcare delivery by providing patient-specific information, giving individuals access to their own health data, helping them interpret those data, supporting communication between themselves and their providers, making people aware of their everyday health behaviors, and supporting healthy behavior changes. Individuals are also demonstrating a growing fascination with "personal health records" (PHRs), which allow them to record health information such as blood pressure, weight, and exercise.[86]

In addition, portable and home healthcare devices—pacemakers, continuous positive airway pressure machines, home dialysis systems, and the like—generate a wealth of real-world, digital data. For example, 200,000 diabetics wear insulin pumps that continuously record blood glucose.[87] Patients upload that information to manufacturer-provided websites for making individual treatment decisions.[88] This information—already being recorded and stored in digital form—would be valuable for assessing the progress of diabetes and recommending better treatments. In our increasingly technology-rich society, many people generate and access recorded data in their everyday lives that are critical for their own care. Ensuring researchers have access to such individual health information could be invaluable for the treatment of patients with similar health profiles, as well as for research into new treatments.

Promoting-Health-Information-Technology.aspx.

84. *See generally* Caitlyn Ross, *Stimulus Bill Funds Overdue Changes to U.S. Health Care Technology*, 37 J.L. MED. & ETHICS 385 (2009).

85. *Mobile HealthCare Applications Represent the Next Frontier in the Life Sciences Industry*, BIOJOBBLOG (Dec. 14, 2010).

86. Janice L. Clarke, Deborah C. Meiris & David B. Nash, *Electronic Personal Health Records Come of Age*, 21 AM. J. MED. QUALITY 5S–15S (3 Supp. 2006).

87. Richard M. Bergenstal et al., *Effectiveness of Sensor-Augmented Insulin-Pump Therapy in Type 1 Diabetes*, 363 NEW ENG. J. MED. 311 (2010); *Diabetes Monitor—Q&A About Pump Therapy*, DIABETESMONITOR.COM (Jan. 6, 2010), http://www.diabetesmonitor.com/b46.htm.

88. *See, e.g.*, MEDTRONIC, CARELINK PERSONAL, GETTING STARTED (2008), http://www.minimed.com/pdf/carelink_personal_getting_started_guide.pdf.

In sum, personal information is vital for health research. It plays a rapidly expanding role in retrospective studies, research subject identification, research protocol development, genetic research and personalized medicine, the evolution of EHRs and PHRs, and cutting edge research based on nontraditional, real-world data. Obtaining access to these valuable data is often a challenge for researchers, however, because of confusion between the norms and legal rules that apply to traditional research and those appropriate for data-based research.

B. Autonomy and Informed Consent

Individual autonomy— "signif[ying] control of decision-making and other activity by the individual"[89]—lies at the heart of modern health care and health law, especially in the United States. This has not always been the case in all countries, and as we move increasingly to a system in which health care is not only paid for by third parties, but actually managed by them as well, it is not clear that it will continue to be the case in the United States. But for the moment, autonomy is the bedrock of medical practice and research. As Justice Benjamin Cardozo asserted in 1914: "Every human being of adult years and sound mind has a right to determine what shall be done with his own body."[90]

The obvious corollary of autonomy is informed consent. If individuals have the right to control what is done with their bodies, they must certainly have the right to be told what the options are and the potential risks and benefits of each. Professor LeBlang wrote that "[i]nformed consent is . . . a core concept central to American beliefs about individual rights and the proper relationship between patients and providers."[91]

In 1979, the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research clearly extended the obligation to provide informed consent to researchers.[92] In its final report, *The Belmont Report*, the Commission identified three overarching principles applicable to research involving human subjects: respect for persons, beneficence, and justice.[93] According to the report, "respect for persons" includes the "ethical conviction" that "individuals should be treated as autonomous agents."[94] The report noted that "[a]n autonomous person is an individual capable of

89. Bart J. Collopy, *Autonomy in Long Term Care: Some Crucial Distinctions*, 28 GERONTOLOGIST 10 (Supp. 1988).

90. Schloendorff v. Soc'y of N.Y. Hosp., 105 N.E. 92, 129 (N.Y. 1914).

91. Theodore R. LeBlang et al., *Informed Consent to Medical and Surgical Treatment*, *in* LEGAL MEDICINE 343, 349 (6th ed. 2004).

92. *See* NAT'L COMM'N FOR THE PROT. OF HUMAN SUBJECTS OF BIOMEDICAL AND BEHAV. RES., DEP'T OF HEALTH, EDUC. & WELFARE, THE BELMONT REPORT: ETHICAL PRINCIPLES AND GUIDELINES FOR THE PROTECTION OF HUMAN SUBJECTS OF RESEARCH (1979) [hereinafter THE BELMONT REPORT], *available at* http://ohsr.od.nih.gov/guidelines/belmont.html.

93. *Id.*

94. *Id.* at 4.

deliberation about personal goals and of acting under the direction of such deliberation. To respect autonomy is to give weight to autonomous persons' considered opinions and choices while refraining from obstructing their actions unless they are clearly detrimental to others."[95]

In the health research context, the key manifestation of respect for persons is informed consent. According to *The Belmont Report*, "Respect for persons requires that subjects, to the degree that they are capable, be given the opportunity to choose what shall or shall not happen to them. This opportunity is provided when adequate standards for informed consent are satisfied."[96]

C. The Common Rule

The Belmont Report's recommendations are reflected in regulations that have been adopted by eighteen federal agencies and are known as the Common Rule.[97] The Common Rule governs most federally funded research conducted on human beings and, as discussed below, establishes the basic requirements applicable to almost all research on human subjects in the United States.[98] The Common Rule includes three basic requirements aimed at protecting research subjects: "a review of proposed research by an Institutional Review Board (IRB), the informed consent of research subjects, and institutional assurances of compliance with the regulations."[99]

Meaningful informed consent is one cornerstone of human subjects' protections. To provide informed consent, a potential research subject must both understand what participation in a study entails (be "informed"), and agree to participate ("consent"). The Common Rule requires that a researcher obtain informed consent, usually in writing, from a living person or their legally authorized representative before the person can be admitted to a study.[100] The Common Rule also requires that researchers provide human subjects with

95. *Id*. at 5.

96. *Id*. at 10.

97. Protection of Human Subjects Rule, 45 C.F.R. pt. 46 (2009). Departments and agencies adopting the Common Rule include: the Department of Health and Human Services, Department of Agriculture, Department of Energy, National Aeronautics and Space Administration, Department of Defense, Consumer Product Safety Commission, International Development Cooperation Agency (Agency for International Development), Department of Housing and Urban Development, Department of Justice, Department of Defense, Department of Education, Department of Veterans' Affairs, Environmental Protection Agency, National Science Foundation, and Department of Transportation. The Common Rule applies to the Central Intelligence Agency by Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981), and the Social Security Administration by Social Security Independence and Improvement Act of 1994, Pub. L. No. 103-296, 108 Stat. 1464. The Office of Science and Technology Policy signed but did not codify the Common Rule, because it does not conduct clinical research. ERIN D. WILLIAMS, CONG. RESEARCH SERV., RL 32909, FEDERAL PROTECTION FOR HUMAN RESEARCH SUBJECTS 6 n.5 (2005), *available at* http://fas.org/sgp/crs/misc/RL32909.pdf.

98. *See* WILLIAMS, *supra* note 97, at 1.

99. *Id.*

100. *Id.*

extensive information when seeking their consent to participate in research.[101]

IRBs generally have the responsibility of ensuring the adequacy of informed consent and overseeing research involving human subjects. IRBs generally review and must approve (or disapprove) federally funded research on human subjects. IRBs must meet certain structural and membership requirements, including having at least five members with different expertise, at least one of whom is not affiliated with the investigator's institution.[102] For proposed research to be approved under the Common Rule, an IRB must find that numerous requirements are satisfied, including that "informed consent is sought from each subject" and "when appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data."[103] For certain types of research, the Common Rule permits evaluation under "expedited review," which usually means review only by the chair of the IRB.[104]

Although the Common Rule applies only to federally funded research, institutions receiving federal support for any nonexempt human subjects research must provide a "Federalwide Assurance" to the federal government

---

101. Researchers must provide subjects with:

- a statement that the study involves research, an explanation of the purposes of the research and the expected duration of the subject's participation, a description of the procedures to be followed, and identification of any procedures which are experimental;
- a description of any reasonably foreseeable risks or discomforts to the subject;
- a description of any benefits to the subject or to others which may reasonably be expected from the research;
- a disclosure of appropriate alternative procedures or courses of treatment, if any, that might be advantageous to the subject;
- a statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained;
- for research involving more than minimal risk, an explanation as to whether any compensation and an explanation as to whether any medical treatments are available if injury occurs and, if so, what they consist of, or where further information may be obtained;
- an explanation of whom to contact for answers to pertinent questions about the research and research subjects' rights, and whom to contact in the event of a research-related injury to the subject; and
- a statement that participation is voluntary, refusal to participate will involve no penalty or loss of benefits to which the subject is otherwise entitled, and the subject may discontinue participation at any time without penalty or loss of benefits to which the subject is otherwise entitled.

45 C.F.R. § 46.116(a) (2009).

102. *Id.* § 46.107.

103. *Id.* § 46.111.

104. *Id.* § 46.110. To qualify for expedited review, projects must either fit within categories defined by the Secretary of HHS and involve "no more than minimal risk," *id.*, or involve only "minor changes in previously approved research during the period (of one year or less) for which approval is authorized." WILLIAMS, *supra* note 97, at 4. The Common Rule defines "minimal risk" as that in which "the probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests." 45 C.F.R. § 46.102(i).

providing information about how they comply with the Common Rule.[105] In its Federalwide Assurance, an institution may "voluntarily extend the Common Rule or 45 CFR part 46 to all research regardless of the source of support."[106] In fact, many research institutions voluntarily comply in order to avoid situations in which one institution conducts federally funded research according to one set of rules and ethical principles and other research according to different rules and principles.[107] Furthermore, although the decision to apply the Common Rule more broadly is voluntary, once it is included in an institution's Federalwide Assurance, it becomes binding.[108]

To summarize, under the principle of autonomy, which is the bedrock of U.S. health law, and under the Common Rule, which governs most research involving humans, health research on human subjects requires the informed consent of the research subjects. The researchers and the IRB overseeing the research must also ensure that "there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data."[109]

III.
THE PRIVACY RULE

Health privacy is protected at the federal level in the United States by the Privacy Rule (the Rule) that HHS issued in 2001 under HIPAA.[110] This Part discusses the details of the Privacy Rule and analyzes the burdens it imposes on health research, in light of the critique of choice made in Part I. Although the Privacy Rule offers three different options for researchers seeking to gain access to personal health information, none of these mechanisms has proved workable in practice.

A. Basic Requirements

As amended in 2002 and again in 2009,[111] the Rule regulates the use of information that identifies, or reasonably could be used to identify, an individual and that relates to physical or mental health, the provision of health care to an individual, or payment for health care.[112] The Rule applies to

105. *Office for Human Research Protections Federalwide Assurance Frequently Asked Questions*, OFFICE FOR HUMAN RESEARCH PROTECTIONS, U.S. DEP'T OF HEALTH & HUMAN SERVS. [hereinafter *Frequently Asked Questions*], http://www.hhs.gov/ohrp/FWAfaq.html (last visited Oct. 14, 2010).

106. *Id.*

107. *Id*. A complete list of all Federalwide Assurances is available at http://ohrp.cit.nih.gov/search/ (last visited Oct. 14, 2010).

108. *Frequently Asked Questions*, *supra* note 105.

109. 45 C.F.R. § 46.111(a)(7).

110. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (codified at 45 C.F.R. pt. 160, §§ 164.502, 164.506).

111. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,181 (Aug. 14, 2002) (codified at 45 C.F.R. pts. 160 & 164).

112. 45 C.F.R. § 164.504.

"covered entities," namely, anyone who provides or pays for health care in the normal course of business.[113]

A covered entity may use personal health information to provide, or obtain payment for, health care only after first providing the patient with notice and making a good faith effort to obtain an "acknowledgment."[114] Notices must meet detailed requirements set forth in the Rule. For example, proof of providing notice and acknowledgments must be retained for six years after the date on which service is last provided.[115]

For most purposes other than treatment or payment, a covered entity may use personal health information only with an individual's opt-in "authorization."[116] An "authorization" must be provided by obtaining an independent document that specifically identifies the information to be used or disclosed, the purposes of the use or disclosure, the person or entity to whom a disclosure may be made, and other information.[117] A covered entity may not require an individual to sign an authorization as a condition of receiving treatment or participating in a health plan.[118] Furthermore, a covered entity may use or disclose personal health information for directories only if the covered entity obtains the "agreement" of the individual.[119] An agreement need not be written, provided that the individual is informed in advance of the use and has the opportunity to opt out of any disclosure.[120]

Despite its many restrictions on the use of personal information, the federal Privacy Rule is only the minimum required regulation. States are free to adopt more stringent protections,[121] including a law that

> prohibits or restricts a use or disclosure in circumstances that would be permitted under HIPAA; . . . provides an individual with a greater amount of information regarding disclosure, rights, and remedies; . . . narrows the scope or duration of any legal permission to use PHI [protected health information], or increases the privacy protections afforded to PHI; . . . [or] provides greater privacy protection for the individual with respect to any other matter.[122]

While the federal health Privacy Rule marks the apex of choice-based U.S. privacy law and the growing complexity of notice and consent requirements, it also allows for even more burdensome state regulation.

---

113. *Id.* § 164.504.
114. *Id.* § 164.506(a).
115. *Id.* § 164.105(c)(2).
116. *Id.* § 164.508(a)(1).
117. *See id.* § 164.508(c).
118. *Id.* § 164.508(a)(2)(iv).
119. *Id.* § 164.510.
120. *Id.*
121. *Id.*, at pt. 160, subpt. B.
122. BEYOND THE HIPAA PRIVACY RULE, *supra* note 24, at 187–88.

B. The Privacy Rule Applied to Health Research

While the Privacy Rule and more stringent state laws aim to protect the privacy of patient health information, that protection threatens the viability of health research. Congress recognized the reality of this threat and the importance of personal information in health research. As a result, Congress signaled its intention that privacy protections not impede researcher access to that information. Two House reports on HIPAA contain identical language to this effect: "As health [care] plans and providers continue to focus on outcomes research and innovation, it is important that the exchange and aggregated use of health care data be allowed."[123]

HHS implemented Congress' intent in the Privacy Rule by permitting the use of protected health information (PHI) for research if one of three conditions is met: (1) the PHI is deidentified; (2) the data subject provides explicit, written consent; or (3) an Institutional Review Board (IRB) or Privacy Board[124] provides consent.[125] All three conditions have proven onerous, and in some cases impossible, to comply with in practice.

1. Deidentification

Under the Privacy Rule, deidentified PHI is "not individually identifiable health information," and therefore is not subject to the Rule's restrictions.[126] Deidentification requires removing eighteen data elements, including not only obvious identifying information, such as name and contact information, but also all geographic subdivisions smaller than a state (except for the initial three digits of a ZIP Code in certain limited circumstances), all date elements other than year, and any biometric identifiers.[127] (There is a variation on the exception for deidentified data for a "limited data set" that has sixteen of the eighteen data elements required for true deidentification removed, but only if the researchers have executed a "data use agreement" restricting the use of the data set.)[128]

---

123. H.R. REP. NO. 104-736, at 265 (1996); H.R. REP. NO. 104-496, pt. 1, at 100 (1996).

124. The Privacy Rule provides for the creation of Privacy Boards, which are created and operate similarly to IRBs, but exist for the sole purpose of reviewing requests for waivers of authorization for health research. 45 C.F.R. § 164.512(i)(1)(B).

125. *See id*. §§ 164.508(a)(1), 164.512(i), 164.514(a).

126. *Id*. § 164.514(a).

127. *Id*. § 164.514(b)(2)(i).

128. *Id*. § 164.514(e)(2). A data use agreement between the covered entity and the limited data set recipient must:

> (A) Establish the permitted uses and disclosures of such information by the limited data set recipient, . . . ;
>
> (B) Establish who is permitted to use or receive the limited data set; and
>
> (C) Provide that the limited data set recipient will:
>
> > (1) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
> >
> > (2) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

The deidentification provisions are useless for most medical research because researchers require access to information about the patient's medical history, the time and date drugs were administered, or other data prohibited under the deidentification standard. Genetic research is impossible under this provision because genetic information is by definition a biometric identifier.[129] As a result, health researchers are required to obtain consent, either by approaching research subjects directly or by obtaining consent from an IRB or Privacy Board on their behalf.

2. Individual Consent

The Privacy Rule permits access to PHI for health research with the written authorization of each individual patient.[130] This authorization is merely to access and use information; it is in addition to whatever other consent is required under applicable federal and state laws to participate in research involving human subjects.[131] While the Privacy Rule may appear to be a reasonable compromise between privacy concerns and research needs, in practice the Rule and its reliance on individual consent impose significant burdens. Most significant among these burdens are: increased costs of research, introduction of selection bias, and limits on the types of studies that may feasibly be conducted.

Under the Privacy Rule, authorization must be "specific and meaningful"[132] and include a "description of each purpose of the requested use or disclosure."[133] HHS has determined that the authorization must be "study-specific."[134] As such, authorization for "future unspecified research" is prohibited.[135] (In July 2010, HHS indicated that it was "considering" modifying this requirement, although as a condition for doing so, it might require additional disclosures.)[136]

---

(3) Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;
(4) Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
(5) Not identify the information or contact the individuals.

Id. § 164.514(e)(4).

129. NANCY LEE JONES & AMANDA K. SARATA, CRS REPORT FOR CONGRESS, GENETIC INFORMATION: LEGAL ISSUES RELATING TO DISCRIMINATION AND PRIVACY 19 (Mar. 10, 2008), *available at* http://assets.opencrs.com/rpts/RL30006_20080310.pdf ("Individually identifiable health information is defined broadly and includes genetic information.").

130. 45 C.F.R. § 164.508(a)(1).

131. *See supra* notes 97–109 and accompanying text.

132. 45 C.F.R. § 164.508(c)(1)(i).

133. *Id.* § 164.508(c)(1)(iv).

134. Standards for Privacy of Individually Identifiable Health Information, *supra* note 111.

135. *Id.* at 53,226.

136. Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40,868, 40,894 (proposed July 14, 2010) (to be codified at 45 C.F.R. pts. 160 & 164).

Obtaining individual consent is problematic for many of the reasons already identified, but it has proved especially difficult in the context of health research under the exacting requirements of the Privacy Rule. Consent is often easiest to obtain at time of admission to a hospital or when the patient is undergoing treatment, but this leads to obstacles with both practical and ethical dimensions.

The person or entity managing the admission or treatment is rarely the same one who will conduct the research, so obtaining consent in advance may require one institution obtaining consent for the research of another. In addition, because the authorization to use personal data for research must be study-specific, it can only be obtained for studies that are already fully developed and have undergone IRB review (since the consent forms require IRB approval). Also, at time of admission to a hospital or during the treatment relationship, patients are often focused on their immediate health care needs and not particularly interested in addressing matters concerning unrelated uses of their health information. Obtaining consent is especially problematic when seeking data for control groups. For example, when a physician asks a healthy individual for permission to include his or her data in a cancer study, this often raises concerns that he or she is being diagnosed with cancer or is at risk for such a condition.[137] Furthermore, there is a significant ethical question about whether it is appropriate to approach patients at time of admission or treatment seeking authorization to use personal data for a study unconnected to their care, or whether any authorization obtained under such stressful circumstances is ethically valid.

The alternative to obtaining authorization at time of admission or during treatment is to seek it at a later date, but this is even more problematic. First, the patient must still be living, which is often not the case, especially when research involves life-threatening conditions. Furthermore, the patient must be located; with forty-five million Americans moving every year, this is easier said than done.[138] Once located, they have to be contacted, which is both expensive and time-consuming. In-person contacts may yield higher consent rates than telephone or mail solicitations, but they are significantly more expensive and can be more burdensome to the individual. This is all necessary just to obtain patients' permission to examine their medical records. For studies with more rigorous selection criteria, hundreds or even thousands of records must be examined just to find one person whose data are relevant.[139] Because consent must be study-specific, this process must be undertaken separately for

137. David Casarett et al., *Bioethical Issues in Pharmacoepidemiologic Research*, *in* PHARMACOEPIDEMIOLOGY 593 (Brian L. Strom ed., 4th ed. 2005).

138. *Addressing*, UNITED STATES POSTAL SERVICE, http://pe.usps.com/businessmail101/addressing/ (last visited Oct. 14, 2010).

139. *See* U.S. GEN. ACCOUNTING OFFICE, GAO/HEHS-99-55, MEDICAL RECORDS PRIVACY 14–15 (1999), *available at* http://www.gao.gov/archive/1999/he99055.pdf.

each research project.

Further compounding the problem of expense is the chilling effect that requiring consent may have on participation rates. David Casarett, Jason Karlawish, Elizabeth Andrews, and Arthur Caplan have noted that

> if individuals must be contacted each time their records may be used in a particular study, the individual may consider such contact intrusive. Furthermore, individuals might consider that their confidentiality has been violated if researchers access research information and contact them directly in order to obtain consent for the use of de-identified records. Individuals may also refuse participation if contacted for a study they consider irrelevant to their health. An individual may also become alarmed if asked to consent for records to be used in such a study of a disease for which she has not been diagnosed. . . .[140]

One 1999 study, conducted before the Privacy Rule took effect and therefore able to compare participation rates in research studies in states with different consent requirements, found that in states where research access to medical records did not require patient authorization, investigators were able to access 93 percent of the potential study population.[141] But in states where consent was required, only 19 percent of the available population participated.[142]

Moreover, the burdens imposed by the Privacy Rule have been clearly shown to introduce selection bias.[143] Some large medical institutions with extensive treatment and research programs, such as the Mayo system, have proved successful in obtaining a high rate of consent.[144] But even there, the 20 percent of people who refuse to consent—or to make a decision of any form—exhibit distinct demographic and health characteristics that are statistically capable of skewing the research base.[145] Jack V. Tu et al. found that requiring consent before adding patient data to the Registry of the Canadian Stroke Network created a database that was "not representative."[146] David Armstrong et al. compared patients who consented to their data being added to the Acute Coronary Syndrome Registry before the enactment of HIPAA (when consent could be obtained by telephone) and post-HIPAA (when consent had to be in writing) and found that

---

140. Casarett et al., *supra* note 137, at 593.

141. Douglas B. McCarthy et al., *Medical Records and Privacy: Empirical Effects of Legislation*, 34 HEALTH SERVICES RES. 417 (1999).

142. *Id.*

143. BEYOND THE HIPAA PRIVACY RULE, *supra* note 24, at 210–14.

144. *See* Steven J. Jacobsen et al., *Potential Effect of Authorization Bias on Medical Record Research*, 74 MAYO CLINIC PROC. 330 (1999).

145. *Id.*

146. BEYOND THE HIPAA PRIVACY RULE, *supra* note 24, at 210 (referring to Jack V. Tu et al., *Impracticability of Informed Consent in the Registry of the Canadian Stroke Network*, 350 NEW ENG. J. MED. 1414 (2004)).

> [p]atients who gave consent post-HIPAA were more likely to be older, married, and white than those who refused to provide consent or did not respond. Patients who gave consent also had lower mortality rates at 6 months than patients who refused consent. The results suggest that implementation of the Privacy Rule led to selection bias in the Registry.[147]

David Casarett et al. noted that even when the refusal rate was as low as 3.2 percent, "the persons declining consent varied from the study population by age, gender, residence, and prior diagnoses, suggesting that the ability to opt out of databases creates a potential bias in the data."[148]

The Privacy Rule's requirement that authorizations for the use or disclosure of PHI include "[a] description of each purpose of the requested use or disclosure" serves to exacerbate the problems associated with consent and may hinder certain types of data-based research.[149] As noted, in the August 2002 final rule, HHS commented that research-related purposes described in the authorization must be "study-specific" and that authorizations for "future unspecified research" would be considered overly broad and invalid.[150] Yet many research uses of health information—for example, for registries and retrospective studies (described in Part II.A above)—are designed to facilitate unforeseen research studies. They provide an efficient, cost-effective tool for conducting research, testing hypotheses, looking for heretofor undiscovered correlations—none of which will be known at the time an individual permits his or her heath data to be added.[151] The study-specific requirement of the Privacy Rule undermines many of the benefits of data-based research and greatly adds to its cost, since consent must be obtained from each individual for each study. The requirement also restricts tissue banking and other forward-looking genetic research models.[152]

The announcement from HHS in July 2010 that it is "considering" modifying the study-specific consent requirement is welcome news.[153] Concerns remain, however, about the fact that the department is only "considering" such a change at this point, and that it has indicated it might require additional disclosures for research involving "genetic analyses or mental health research" as a condition of such a change—thus adding to the

147. *Id*. at 213 (referring to David Armstrong et al., *Potential Impact of the HIPAA Privacy Rule on Data Collection in a Registry of Patients with Acute Coronary Syndrome*, 165 ARCHIVES INTERNAL MED. 1125 (2005)).

148. Casarett et al., *supra* note 119, at 594.

149. 45 C.F.R. § 164.508(c)(1)(iv) (2009).

150. Standards for Privacy of Individually Identifiable Health Information, *supra* note 111, at 53,226.

151. *See supra* notes 61–87 and accompanying text.

152. BEYOND THE HIPAA PRIVACY RULE, *supra* note 24, at 164, 208–09, 287.

153. Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act, 75 Fed. Reg. 40,868, 40,894 (proposed July 14, 2010) (to be codified at 45 C.F.R. pts. 160 & 164).

mound of legal disclosures that few individuals read.[154] These terms are ill-defined and could lead to confusion, especially since even characteristics such as "gender" are determined genetically, so that research to determine if a condition disproportionately affects women could be considered "genetic analyses" and would require additional stipulations in the authorization document.

The burden on research imposed by the Privacy Rule is in addition to that imposed by the Common Rule, which applies to all federally funded research involving human subjects.[155] Because the consent requirements of the Common Rule and the Privacy Rule differ in significant ways, researchers are likely to face overlapping or redundant requirements. For example, the rules define PHI and deidentification differently.[156] Under the Common Rule, researchers are permitted to collect data, as well as biological samples from which data are derived, for unspecified future uses, "as long as any unintended use is described in sufficient detail to allow informed consent";[157] the Privacy Rule forbids this.[158] And the Common Rule takes a far more permissive view towards deidentification, requiring only that the "the identity of the subject may not be readily ascertained by the health researcher," while the HIPAA Privacy Rule is much more restrictive.[159]

These and other inconsistencies between the Privacy Rule and the Common Rule further complicate the conduct of health research, increase its costs, and introduce considerable uncertainty into health research. Yet the overlap and inconsistency between the two rules affords individuals with no greater privacy protection.

In sum, the Privacy Rule's individual consent provisions as applicable to research have not proved to be workable or desirable in many settings. They raise ethical concerns for patients and severely hinder medical research by imposing additional costs, introducing selection biases, and imposing limitations on the types of research that may be conducted.

3. IRB Substituted Consent

The alternative to individual authorization for the use of personal information in health research is to persuade an IRB or Privacy Board to substitute its consent for that of the data subject.[160] The Privacy Rule permits an IRB or Privacy Board to waive the need for individual authorization only if three conditions are met: (1) the use or disclosure of protected health

154. *Id.*
155. 45 C.F.R. pt. 46.
156. *See id.* § 46.102(f)(2).
157. BEYOND THE HIPAA PRIVACY RULE, *supra* note 24, at 45.
158. *See* 45 C.F.R. §§ 164.508(c)(1), 164.514(b).
159. *See id.* § 46.102(f)(2).
160. *Id.* § 164.512(i)(1)(i).

information involves no more than "minimal risk" to the privacy of individuals; (2) the "research could not practicably be conducted" without the waiver or alteration; and (3) the "research could not practicably be conducted without access to and use of the protected health information."[161] While two of these conditions concern "practicability," the Privacy Rule does not define this term and offers "no guidance as to what factors (e.g., feasibility or cost) should be considered in determining whether the criteria are met."[162]

The third requirement regarding "minimal risk" is similarly ambiguous and problematic.[163] "Minimal risk," as we have already seen in the context of the Common Rule, means that "the probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests."[164] It is difficult to determine what this means when applied to personal information, precisely because the HIPAA Privacy Rule requires individual consent even in situations in which no "harm or discomfort" is threatened.[165] In addition, the Privacy Rule identifies three elements that must be in place to satisfy the "minimal risk" requirement. The first of these is an "adequate plan to protect the identifiers from improper use and disclosure."[166] The second required element is an "adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law."[167] The final required element is "[a]dequate written assurances that the protected health information will not be reused or disclosed to any other person or entity."[168]

In sum, IRBs are charged by law with two primary tasks: balancing the potential benefits of proposed research with the risk to the research subject, and ensuring that the researchers obtain the informed consent of the research subjects. Their members bring their diverse and professional judgment to ensure both that the benefits and risks are adequately described to the research subject and that the request being made to the data subject is objectively reasonable. Unlike most privacy laws, under the Common Rule, consent is only an answer if the question being asked is reasonable. Yet Casarett et al. have noted, "[t]he risks to the subjects of epidemiology research are not the usual health risks of research that can be balanced against the potential health benefits of research."[169] Instead, "the chief risk is a violation of confidentiality,

161. *Id.* § 164.512(i)(2)(ii).
162. BEYOND THE HIPAA PRIVACY RULE, *supra* note 24, at 169.
163. 45 C.F.R. § 164.512(i)(2)(ii)(A).
164. *Id.* § 46.102(i).
165. *See* 45 C.F.R. § 164.508(a).
166. *Id.* § 164.512(i)(2)(ii)(A).
167. *Id.*
168. *Id.*
169. Casarett et al., *supra* note 137, at 597.

which is really a civil, rather than a medical, risk."[170] And often those are risks that IRBs are neither familiar nor experienced with resolving.

The Privacy Rule prohibits the use of personal health data for research unless one of three conditions is met. The first is deidentification, which makes the data useless for the vast majority of research.[171] The second is individual consent, which is often time-consuming and expensive, burdensome to individuals, ethically questionable, and runs the risk of introducing selection bias if even a small percentage of the population declines.[172] Moreover, because of restrictive HHS interpretations and unlike the requirements of the Common Rule, consent is unavailing for future unspecified research, as is often the case with data-based research. Researchers are therefore left with the third option: IRB substituted consent—the alternative with the greatest flexibility, but one that challenges the capabilities of most IRBs.[173] As a result, the overarching effect of the Privacy Rule is to impose a substantial burden on data-based health research and provide problematically weak protection of personal health information.

IV.
THE IMPACT OF CHOICE ON HEALTH RESEARCH AND PRIVACY

The Privacy Rule imposes a considerable burden on health research in large part because of its reliance on individual choice. Unless personal health information is completely deidentified, which makes it useless for the vast majority of health research, it can only be used with the explicit consent of the individual or with the substituted consent of an IRB.

In 2007, the IOM convened a Committee on Health Research and the Privacy of Health Information, which issued its final report in February 2009.[174] After documenting many of the issues outlined above, the committee reached two broad conclusions: "the HIPAA Privacy Rule does not protect privacy as well as it should" and "as currently implemented, the HIPAA Privacy Rule impedes important health research."[175] In reaching these conclusions, the IOM committee reflected similar conclusions reached by earlier studies.[176] To take just one example, in 2003 the Association of American Medical Colleges created a database of experiences with HIPAA and reported the "most common effects of the Privacy Rule on health research" to be:

(1) reduced patient recruitment, (2) increased the likelihood of

170. *Id.*
171. *See supra* notes 126–128 and accompanying text.
172. *See supra* notes 131–159 and accompanying text.
173. *See supra* notes 160–168 and accompanying text.
174. BEYOND THE HIPAA PRIVACY RULE, *supra* note 24, at 67–70.
175. *Id.* at 2.
176. *Id.* at 199–209.

> selection bias, (3) increased the costs of conducting research by requiring more paperwork and complicating the IRB approval process, (4) increased the number of errors in research when deidentified information was used, (5) made multisite trials more difficult because of variations in IRB interpretation of the Rule, and (6) caused researchers to abandon projects because of the increased number of rules for operating a research study.[177]

The IOM committee documented serious problems created by the Privacy Rule's consent requirements, including difficulties with recruiting participants, selection bias, cost and efficiency, and inter-institutional collaboration.[178] Ultimately, the committee concluded that consent requirements not only make health research more expensive, less efficient, and less accurate, but also that potentially important research studies are actually abandoned.[179] While the burden placed on health research by the Privacy Rule is considerable today, it will only become more acute as the use of EHRs, PHRs, and other data expands and research becomes even more information-based and more individualized.[180]

More importantly, the burdens imposed by the Privacy Rule's consent requirement on medical research do not advance privacy. As the IOM panel wrote: "consent (authorization) itself cannot achieve the separate aim of privacy protection."[181] The committee's reasoning is clear and stark: the "obligations to safeguard privacy, such as security, transparency, and accountability, are independent of patient consent. In fact, preventing the secondary use of personal data is the only privacy obligation that consent can potentially address."[182]

The Privacy Rule's reliance on consent, far from being justified on any ethical basis, actually poses significant ethical issues. For example, by relying on patient authorization for the use of data in health research, we ignore the fact that "few patients are sufficiently informed to make educated decisions about how their data should be used."[183] Similarly, we are presenting choices to patients knowing that "many consumers do not read the details of informed consent forms" and that "even when they do read the forms, they often do not comprehend all the details."[184] The Privacy Rule ignores the strong evidence that "many consumers mistake the existence of any privacy policy for a

177. *Subcomm. on Privacy and Confidentiality*, *National Comm. on Vital and Health Statistics* (Nov. 19, 2003) (testimony of Susan Ehringhaus, Associate General Counsel for the Association of American Medical Colleges).

178. *See* BEYOND THE HIPAA PRIVACY RULE, *supra* note 24, at 209–30.

179. *Id.*

180. See *id*. at 254.

181. *Id*. at 250.

182. *Id*.

183. *Id*. at 251.

184. *Id*.

guarantee that information will be strongly protected and withheld from outside persons, even if the consent says differently."[185] Moreover, the rule causes us to ask patients to "give informed consent at a time when they are not in good health and are not motivated or lack the ability to make these kinds of complicated decisions."[186]

Consent requirements not only impede health research, but may actually undermine privacy interests. As discussed in Part III.B.2, "if individuals must be contacted each time their records may be used in a particular study in order to obtain informed consent, as the Privacy Rule requires, such contact could be considered intrusive and counter to the tenets of confidentiality."[187] The challenge is especially great when individuals are asked to have their data included in a study as part of the control sample—i.e., data about people who do not have the condition that is being studied.

There is a still stronger ethical objection to the Privacy Rule's reliance on consent for examining personal information in health research. Helena Gail Rubinstein, a former Director of Policy Analysis and Program Development in the Massachusetts Group Insurance Commission, has written that "while autonomy is an appropriate framework for evaluating questions concerning the treatment of one's body, it is not the appropriate framework for evaluating rules to regulate the use of health data."[188] Ms. Rubinstein further stated that relying on consent refuses to recognize, "in exchange for the vast improvements in medical care, a correlative responsibility on the part of the individual, as a potential consumer of health care services, toward the community." She concluded: "As individuals rely on their right to be let alone, they shift the burden . . . for providing the data needed to advance medical and health policy information. Their individualist vision threatens the entire community."[189]

Ironically, it may be questionable to speak of "their individualist vision," because this vision is largely the creation of regulators at HHS, not of research subjects. Polling data show public support for the responsible use of personal data for health research, subject to appropriate deidentification, transparency requirements, and strong legal oversight.[190]

Moreover, the insistence on choice is itself a choice. The Privacy Rule provides for no individual choice concerning uses of personal information that HHS believes are so important as to outweigh privacy concerns. Nonconsensual

185. *Id*.
186. *Id*.
187. *Id*. at 252.
188. Helena Gail Rubinstein, *If I Am Only for Myself, What Am I? A Communitarian Look at the Privacy Stalemate*, 25 AM. J.L. & MED. 203, 223 (1999).
189. *Id*. at 226.
190. *See, e.g*., David M. Haas et al., *Patient Attitudes Toward Genotyping in an Urban Women's Health Clinic*, 112 OBSTETRICS & GYNECOLOGY 1023 (2008); Paul R. Helft et al., *Cancer Patients' Attitudes Toward Future Research Uses of Stored Human Biological Materials*, 2 J. EMPIRICAL RES. ON HUM. RES. ETHICS 15 (2007).

disclosures of health information are permitted for public health activities; to report victims of abuse, neglect, or domestic violence; in judicial and administrative proceedings with a court order, subpoena, or discovery request; to enable product recalls, repairs, or replacement; to facilitate organ and tissue transplantation; and for law enforcement activities with a warrant, a subpoena, an administrative request, an investigative demand, or even a law enforcement official's request.[191] In these settings, there are no meaningful limits on subsequent use, no anonymization requirements, no security standards, and no provisions for oversight. It is unclear by what ethical principle HHS determined that consent was not required for these uses, but was necessary for the use of personal data in health research.

V.
WAYS FORWARD

There are many positive steps that could reduce the burden on health research created by the Privacy Rule's insistence on choice—whether supplied by the individual or substituted by an IRB. Some approaches would simply make choice work better, while others would diminish the role of choice altogether.

To help make choice work more effectively, for example, regulators could amend the Privacy Rule to bring its requirements into line with those of the Common Rule concerning the definition of PHI,[192] the meaning of deidentification,[193] and the scope of consent.[194] This would at least eliminate the inconsistency that presently imposes additional costs and delays on health researchers without providing any additional benefits to individuals. A second useful approach would be to expand the scope of consent so that individuals could consent to unspecified future uses of health data.[195] The current prohibition on broad consent is found neither in HIPAA nor the Privacy Rule, but rather is an interpretation by the HHS Office of Civil Rights.[196] The burden of that interpretation grows more acute as genetic and large-scale, data-based research expands. HHS could go beyond "considering" reversing this restrictive interpretation, to explicitly permitting authorizations for unspecified future research, consistent with the Common Rule.

Choice could also be made to work better by revising the definition of "deidentified,"[197] so that personal data would not be subject to the Privacy Rule if immediately identifying information (e.g., name, address, Social Security Number) had been removed, and the researcher was prohibited from reidentifying or

191. *See* 45 C.F.R. § 164.512 (2009).
192. *See id*. §§ 164.508, 164.514(b).
193. *Id*. § 46.102(f)(2).
194. BEYOND THE HIPAA PRIVACY RULE, *supra* note 24, at 45; *see also* 45 C.F.R. §§ 164.508, 164.514(b).
195. *See* 45 C.F.R. §§ 164.508, 164.514(b).
196. 67 Fed. Reg. 53181, 53226.
197. *See id*. § 164.514(b)(2)(i).

attempting to identify the data subject, except as required by law. This is a more workable approach to deidentification than the Privacy Rule's current approach, which requires removing so much information as to make the underlying data useless for most research purposes. Moreover, it reflects the reality that, in the face of modern digital technologies, no personal information is ever truly deidentified if it is to retain value for researchers.[198]

A fourth approach would be to move to a more proportional, risk-based concept of consent, so that explicit, written consent is only necessary where serious harm is threatened; other uses of personal data might be permitted with oral consent or even opt-out consent.[199] This would introduce a commonsense proportionality by imposing greater impediments only when greater perceived risks warrant them.

These and similar approaches help reduce the burden imposed by choice on health research and may help make choice more meaningful, but they do little to address the ethical issues raised by requiring choice, in any form, for the use of personal information in health research. Other approaches would diminish the role of individual choice altogether, either by eliminating it entirely in certain circumstances or by creating workable alternatives. Four options appear particularly promising.

The first option is to add IRB-approved health research to the long list of uses of PHI for which the Privacy Rule does not require individual consent. There is ample reason to think that most health research has as much, or even broader, social utility as public health reporting or complying with subpoenas or administrative demands.[200] This approach offers the advantage of fitting easily within the existing structure of the Privacy Rule. It might, however, be criticized as providing too little privacy protection since the Privacy Rule effectively exempts from further direct regulation its long list of uses of PHI that do not require consent.

A second approach would be for HHS and other federal regulators to eliminate the Privacy Rule's consent requirement for use of PHI in health research, but expand the Common Rule to apply to all research involving human subjects, irrespective of the funding source. Because of the terms of many institutions' Federalwide Assurances,[201] such an extension may merely codify existing practice. This approach would avoid unnecessary regulatory duplication and inconsistency, but it would require amending not only the Privacy Rule, but also the Common Rule.

198. *See, e.g.*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

199. Proportionality is a key concept under the Common Rule and in other nations' privacy laws. *See* Casarett et al., *supra* note 137, at 597; BEYOND THE HIPAA PRIVACY RULE, *supra* note 24, at 263.

200. *See* 45 C.F.R. § 164.512.

201. *See supra* notes 105–108 and accompanying text.

The third alternative would be for personal information to be provided to "licensed" or "registered" research facilities without any individual consent, but subject to strict privacy protections. These protections might include strong security requirements, prohibitions on reidentifying information from which name or address had been removed, and effective oversight and enforcement provisions (such as regular privacy audits). These facilities would be restricted by law or contract from using health data provided without individual consent for any research that had not received IRB approval and/or other guarantees of the research's likely social value. This would require substantial new regulation, but that would offer the benefit of clear, specific privacy rules applicable to the research setting.

Finally, personal information could be deposited in "licensed" or "registered" data centers, where they could be accessed for meritorious, IRB-approved research without any individual consent. The data centers would be subject to strict requirements and oversight, as described above, and would provide data to "accredited" research institutions subject to similar conditions. Ontario, Canada, follows a similar approach in its Personal Health Information Protection Act.[202] Richard Thomas, former Information Privacy Commissioner of the United Kingdom, and Mark Walport also recommended a similar approach to the Prime Minister in 2008.[203] As with the prior approach, new regulations would be necessary, but this alternative offers potentially greater data protection by limiting the distribution of PHI. One useful model in U.S. law is the Fair Credit Reporting Act, which imposes strict requirements on "Consumer Reporting Agencies," which are then allowed to collect consumer financial data without individual consent, but can only provide them to end users for "permissible purposes" and subject to important restrictions on their disclosure and use.[204]

The goal here is not to propose a specific solution to the significant problems created by the consent requirements of the Privacy Rule, but rather to demonstrate that there are alternatives that would enhance both health research and personal privacy. In addition, it is critical to recognize that there is no ethical requirement for individual consent (or substituted IRB consent) before personal information is used for health research. Unlike the situation in which research is conducted on the *person*, in which case modern ethics and U.S. law would virtually always require the consent of the individual, the use of personal *data* presents a different situation governed by different ethical norms. As discussed above, those norms require

202. Personal Health Information Protection Act, S.O. 2004, c.3, schedule A (Can.), *available at* http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm; *see also* INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, A GUIDE TO THE *Personal Health Information Protection Act* (2004), *available at* http://www.ipc.on.ca/images/Resources/hguide-e.pdf (explaining the operation of the Ontario health privacy law).

203. RICHARD THOMAS & MARK WALPORT, DATA SHARING REVIEW 70–71 (2008), *available at* http://www.justice.gov.uk/reviews/docs/data-sharing-review-report.pdf.

204. 15 U.S.C. § 1681(a) (2006).

considering not only the potential benefits to individuals and society if health data are used—versus the potential harm to the individual if they are not—but also the wide range of issues surrounding the consent process, the extent to which consent is even practical, the burden on individuals of requesting consent, the effect on the whole data set of even a few individuals declining consent, and the cost in economic and human terms of requiring consent. Those norms also require considering the range of tools for reducing the risk associated with the use of health data—for example, by requiring the removal of names or other readily identifying information, or enacting strong legal protections against reidentifying or reusing health data—and evaluating the extent to which requiring consent actually protects privacy more effectively than these and other regulatory and technological tools. Finally, those norms might also be considered in the context of the numerous other purposes for which federal law permits health data to be used without consent.

Even if an ethical imperative for consent to the use of personal data did exist, it would not be absolute. Instead, as *The Belmont Report* itself recognized, "to repudiate [a] person's considered judgments, to deny an individual the freedom to act on those considered judgments, or to withhold information necessary to make a considered judgment," only shows "lack of respect for an autonomous agent" and would therefore be ethically impermissible if "there are no compelling reasons to do so."[205] This is presumably the logic that undergirded HHS's decision to exempt so many uses of health information from the Privacy Rule.[206] The converse of this principle is true as well. Where a compelling reason to act exists, the decision to wait for consent poses ethical issues. These issues are exacerbated where the benefits to society of using the data are great, as they often are with health research, and where the potential harms to individual data subjects are slight, as they would be in the case of anonymized information being used subject to strong security and nondisclosure protections.

What seems inescapably clear is that the Privacy Rule's requirement of consent cannot be ethically justified on the basis that it protects privacy because, as shown, consent does not equate with privacy. One clear advantage of moving away from a consent-based approach is that it would highlight the urgency of assuring that the law provides the appropriate incentives to ensure that personal privacy is protected.

CONCLUSION

Data protection laws today often regard individual choice as both a tool for protecting privacy and, in some cases, the objective of those laws. This is a serious error in part because choice is rarely effective in protecting privacy, and will only become less so as new technologies and applications increase the supply of, and the demand for, personal information. But it is also a mistake

205. THE BELMONT REPORT, *supra* note 92, at 4.
206. *See* 45 C.F.R. § 164.512 (2009).

because maximizing individual choice is not the same thing as protecting privacy. Laws that confuse the two not only fail to protect privacy, but also frequently undermine other important activities and values as well.

This is clearly the case for health research that uses personal data, which the HIPAA Privacy Rule requires be conducted either with completely deidentified—and therefore generally useless—data, or with consent provided either by individual data subjects or an IRB (or Privacy Board). The result has been a failure to protect individual privacy adequately and a significant impediment to research that could save or dramatically enhance human life. Many of the reasons for these twin failures are practical, and have to do with the difficulty and cost of obtaining consent at any time, as well as the duplication and inconsistency between the Privacy Rule and the Common Rule. But there are also substantial conceptual and ethical objections to relying so heavily on individual choice for access to data for health research.

Autonomy and informed consent are vital ethical and legal principles undergirding the U.S. approach to health care and to health research that involves experimentation on human subjects. But these principles are implicated less strongly, if at all, by data-based health research—research that is becoming more common and more important as more patient data is captured and stored electronically and as the search for personalized therapies increases the volume of data necessary for effective research. In short, there is no ethical principle that requires choice as the basis for research involving patient data, especially if identifying information is masked and the use of the data is subject to strong, substantive security and privacy requirements. Regulatory insistence on choice is quite literally allowing people to die and suffer unnecessarily without even providing the benefit of aiding privacy.

While the burden of choice and its inadequacy for protecting privacy is especially clear in the case of health research, the conclusion applies in other areas as well. Individual choice does not protect privacy in financial transactions, online commerce, or other settings any better than it does in health care. Instead, protecting privacy requires a broad range of tools, such as the eight principles included in the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*,[207] which are the basis for almost all of the national and regional

207. ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *supra* note 2. The eight principles are:

> 1. Collection Limitation Principle—There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
> 2. Data Quality Principle—Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
> 3. Purpose Specification Principle—The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each

privacy regimes that have been adopted since 1980.[208] The valuable activities impeded by choice are not limited to health research.

Recognizing the limits of choice, and notice to facilitate it, does not mean that notice and choice play no role in protecting privacy—in health research or any other setting. Notice can help facilitate transparency, which is critical if the public is to support and fund health research. Similarly, choice grows more appropriate as real harms are threatened or in situations where there are meaningful decisions to be made. But it is time we recognize that in most settings, choice is neither the best tool for protecting our privacy nor an appropriate goal of our privacy laws.

---

occasion of change of purpose.

4. Use Limitation Principle—Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: (a) with the consent of the data subject; or (b) by the authority of law.
5. Security Safeguards Principle—Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
6. Openness Principle—There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. Individual Participation Principle—An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
8. Accountability Principle—A data controller should be accountable for complying with measures which give effect to the principles stated above.

Id. at 14–16.

208. *See, e.g.*, Council Directive 95/46, *supra* note 3; FEDERAL TRADE COMMISSION, *supra* note 13; Asia-Pacific Economic Cooperation, *supra* note 7.